日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月１８日

出願番号
Application Number: 特願２００３－１７３９８５

[ST. 10/C]: [ＪＰ２００３－１７３９８５]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７５８７

【書類名】　特許願
【整理番号】　14313401
【提出日】　平成15年 6月18日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　1/00
【発明の名称】　送信装置、受信装置、送信制御プログラム及び受信制御プログラム
【請求項の数】　21
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
【氏名】　斉　藤　　健
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
【氏名】　磯　崎　　宏
【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝　府中事業所内
【氏名】　加　藤　　拓
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝　青梅事業所内
【氏名】　小久保　　隆
【特許出願人】
【識別番号】　000003078
【住所又は居所】　東京都港区芝浦一丁目１番１号
【氏名又は名称】　株式会社　東　芝

【代理人】

【識別番号】　100075812

【弁理士】

【氏名又は名称】　吉　武　賢　次

【選任した代理人】

【識別番号】　100088889

【弁理士】

【氏名又は名称】　橘　谷　英　俊

【選任した代理人】

【識別番号】　100082991

【弁理士】

【氏名又は名称】　佐　藤　泰　和

【選任した代理人】

【識別番号】　100096921

【弁理士】

【氏名又は名称】　吉　元　弘

【選任した代理人】

【識別番号】　100103263

【弁理士】

【氏名又は名称】　川　崎　康

【先の出願に基づく優先権主張】

【出願番号】　特願2003- 58927

【出願日】　平成15年 3月 5日

【手数料の表示】

【予納台帳番号】　087654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0102514

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　送信装置、受信装置、送信制御プログラム及び受信制御プログラム

【特許請求の範囲】

【請求項１】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含むRTP（Real-time Transport Protocol）ヘッダと、を有するパケットの送信を制御する送信制御手段と、

受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、

前記受信装置との間で、著作権保護のための認証・鍵交換処理を行う認証・鍵交換処理手段と、を備えることを特徴とする送信装置。

【請求項２】

前記認証・鍵交換処理手段は、ネゴシエーションされた前記ペイロードタイプの値を含むパケットが前記受信装置に送信された後に、前記認証・鍵交換処理を行うことを特徴とする請求項１に記載の送信装置。

【請求項３】

前記送信制御手段は、前記認証・鍵交換処理手段による認証・鍵交換に成功した場合に限り、ネゴシエーションされた前記ペイロードタイプの値を含むパケットを前記受信装置に送信することを特徴とする請求項１に記載の送信装置。

【請求項４】

著作権保護を図る必要のある前記パケットを前記受信装置に送信した後、前記パケットが著作権保護を図る必要があることを報知する情報を前記受信装置に送信する著作権保護報知手段を備えることを特徴とする請求項１～３のいずれかに記載の送信装置。

【請求項５】

著作権保護を図る必要のある前記パケットを前記受信装置に送信する前に、前記パケットが著作権保護を図る必要があることを報知する情報と、前記パケット

の暗号フレームサイズとを、前記受信装置に通知する暗号化情報通知手段を備えることを特徴とする請求項１～４のいずれかに記載の送信装置。

【請求項６】

前記受信装置から送信された、著作権保護を図る必要のある前記パケットの暗号フレームサイズを受信する暗号フレームサイズ受信手段と、

前記パケットを、前記暗号フレームサイズ受信手段で受信された暗号フレームサイズにて暗号化する暗号化手段と、を備えることを特徴とする請求項１～５のいずれかに記載の送信装置。

【請求項７】

前記暗号フレームサイズ受信手段により受信された暗号フレームサイズで前記パケットを送信できるか否かを示す暗号フレームサイズ応答を前記受信装置に送信する暗号フレームサイズ応答送信手段を備えることを特徴とする請求項６に記載の送信装置。

【請求項８】

前記ペイロードタイプの値は、２種類以上の値、あるいは所定の範囲内の任意の値であることを特徴とする請求項１～７のいずれかに記載の送信装置。

【請求項９】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含むRTP（Real-time Transport Protocol）を付加したパケットの受信を制御する受信制御手段と、

送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、

前記送信装置との間で、著作権保護のための認証・鍵交換処理を行う認証・鍵交換処理手段と、を備えることを特徴とする受信装置。

【請求項１０】

前記認証・鍵交換処理手段は、ネゴシエーションされた前記ペイロードタイプの値を含むパケットが前記受信装置に送信された後に、前記認証・鍵交換処理を行うことを特徴とする請求項９に記載の受信装置。

【請求項１１】

前記受信制御手段は、前記認証・鍵交換処理手段による認証・鍵交換に成功した場合に限り、ネゴシエーションされた前記ペイロードタイプの値を含むパケットを受信することを特徴とする請求項９に記載の受信装置。

【請求項１２】

前記著作権保護制御データは、電子データを暗号化するための暗号鍵を生成するのに用いられるシード値の少なくとも一部のビットを含んでおり、

前記シード値を用いて、受信された前記パケットに含まれる暗号化された電子データを復号する復号手段をさらに備えることを特徴とする請求項９～１１のいずれかに記載の受信装置。

【請求項１３】

前記送信装置が送信した電子データに含まれる前記シード値に基づいて、前記送信装置がシード値を更新したか否かを判断する更新判断手段と、

前記送信装置がシード値を更新したと判断される場合に、前記送信装置に対して認証・鍵交換要求を送信する認証・鍵交換要求手段と、を備えることを特徴とする請求項１２に記載の受信装置。

【請求項１４】

著作権保護を図る必要のある前記パケットを受信した後、前記パケットが著作権保護を図る必要があることを報知する情報を受信する著作権保護情報受信手段を備えることを特徴とする請求項９～１３のいずれかに記載の受信装置。

【請求項１５】

著作権保護を図る必要のある前記パケットを受信する前に、前記パケットが著作権保護を図る必要があることを報知する情報と前記パケットの暗号フレームサイズとを受信する暗号化情報受信手段を備えることを特徴とする請求項９～１４のいずれかに記載の受信装置。

【請求項１６】

著作権保護を図る必要のある前記パケットの暗号フレームサイズを送信する暗号フレームサイズ送信手段を備えることを特徴とする請求項９～１５のいずれかに記載の受信装置。

【請求項１７】

前記暗号フレームサイズ送信手段が送信した暗号フレームサイズで前記送信装置が電子データを暗号化できるか否かを示す暗号フレームサイズ応答を受信する暗号フレームサイズ応答受信手段を備えることを特徴とする請求項１６に記載の受信装置。

【請求項１８】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含むRTP（Real-time Transport Protocol）ヘッダと、を有するパケットの送信を制御するステップと、

受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うステップと、

前記受信装置との間で、著作権保護のための認証・鍵交換処理とを行うステップと、を備えることを特徴とする送信制御プログラム。

【請求項１９】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含むRTP（Real-time Transport Protocol）を付加したパケットの受信を制御するステップと、

送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うステップと、

前記送信装置との間で、著作権保護のための認証・鍵交換処理とを行うステップと、を備えることを特徴とする受信制御プログラム。

【請求項２０】

著作権保護を図る必要のある前記パケットを前記受信装置に送信する前に、前記パケットをマルチキャストにて送信するか否かを判別するマルチキャスト送信識別手段と、

前記パケットをマルチキャストのパケットにて送信する場合には、前記パケットをマルチキャストの暗号フレームサイズにて暗号化して送信するマルチキャスト暗号化手段と、を備えることを特徴とする請求項１～８のいずれかに記載の送信装置。

【請求項２１】

著作権保護を図る必要のある前記パケットを受信した場合、マルチキャストのパケットであるか否かを判別するマルチキャスト受信識別手段と、

前記パケットがマルチキャストのパケットであると判別された場合には、前記パケットをマルチキャストの暗号フレームサイズにて復号化するマルチキャスト復号化手段と、を備えることを特徴とする請求項９～１７のいずれかに記載の受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、著作権保護を図る必要の電子データを送信または受信する送信装置、受信装置、送信制御プログラム及び受信制御プログラムに関する。

【０００２】

【従来の技術】

デジタル情報家電と呼ばれる商品が増加している。これら商品は、デジタル放送の開始などに伴い、普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレイヤ、ハードディスクレコーダ等のデジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。

【０００３】

この際、考慮すべきは著作権保護である。デジタルデータは、コピー時の品質劣化が無いなどの利点がある反面、容易に不正コピーを行えるなどの欠点も持つ。このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機構や、データの暗号化の機能が兼ね備えられている（非特許文献１参照）。

【０００４】

さて、近年、IEEE1394に加えて、家庭内でパーソナルコンピュータ（以下、PC）を用いたネットワーク（イーサネットや無線LAN等）を手軽に構築できるようになった。これは、PCの普及、ブロードバンド環境の低価格化、ネットワーク対応の機器やソフトウェアの普及など、複数の理由が考えられよう。この流れに、AV機器も加わる可能性がある。

【０００５】

このような環境で利用されるプロトコルは、主にIP（インターネットプロトコル）である。

【０００６】

【非特許文献１】

http://www.dtcp.com

【０００７】

【発明が解決しようとする課題】

しかしながら、インターネットプロトコル自体は著作権保護を特に考慮に入れていないため、AVデータの著作権保護が十分に図れないおそれがある。特に、最近のように、無線LANやBluetooth等の無線ネットワークが普及している状況では、著作権保護の必要なAVデータが無断で複製や再生される可能性が高くなる。

【０００８】

本発明は、このような点に鑑みてなされたものであり、その目的は、著作権保護を図りつつAVデータの送信または受信を行える送信装置、受信装置、送信制御プログラム及び受信制御プログラムを提供することにある。

【０００９】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含むRTP（Real-time Transport Protocol）ヘッダと、を有するパケットの送信を制御する送信制御手段と、受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、前記受信装置との間で、著作権保護のための認証・鍵交換処理とを行う認証・鍵交換処理手段と、を備える。

【００１０】

また、本発明は、暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含むRTP（Real-time Transport Protocol）を付加したパケットの受信を制御する受信制

御手段と、送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、前記送信装置との間で、著作権保護のための認証・鍵交換処理とを行う認証・鍵交換処理手段と、を備える。

【００１１】

【発明の実施の形態】

以下、本発明に係る送信装置、受信装置、送信制御プログラム及び受信制御プログラムについて、図面を参照しながら具体的に説明する。

【００１２】

以下では主に、音声や映像のAVデータを送受する例を説明するが、本発明は、AVデータ以外の各種電子データに適用可能である。

【００１３】

（第１の実施形態）

図１は本発明の一実施形態である送信装置と受信装置とを備えたAV通信システムの概略構成を示すブロック図である。図１のAV通信システムは、ある家庭内のホームネットワーク１と、このホームネットワーク１に接続されている送信装置２及び受信装置３とを備えている。ホームネットワーク１の一例として、以下では無線ネットワーク１について説明するが、無線ネットワーク１の代わりに、あるいは無線ネットワーク１と並行して、イーサネットやIEEE1394等の有線ネットワークを用いてもよい。無線ネットワーク１の具体的な形態は特に問わないが、例えば、IEEE802.11a、IEEE802.11bまたはIEEE802.11gなどの各種の無線LANが考えられる。

【００１４】

送信装置２と受信装置３は、AVデータのやり取りを行う。送信装置２は、セットトップボックスやDVDプレイヤ等のAVデータの送信装置となりうる機器である。受信装置３は、テレビ、表示装置、スピーカ、AV録画・録音装置などのAVデータの受信装置となりうる機器である。

【００１５】

図２は送信装置２の内部構成の一例を示すブロック図である。図２の送信装置２は、インタフェース部１１と、AVデータ生成／蓄積部１２と、RTP（Real-time

Transport Protocol）処理部１３と、著作権保護暗号化部１４と、パケット処理部１５と、通信処理部１６と、著作権保護認証・鍵交換部１７と、AV制御部１８とを有する。

【００１６】

インタフェース部１１は、無線ネットワーク１に接続される部分であり、無線ネットワーク１に対してAVデータ等を送信する。AVデータ生成／蓄積部１２は、受信装置３に送信するためのAVデータの生成や蓄積を行う。RTP処理部１３は、タイムスタンプ処理やシーケンス番号処理などのトランスポート層層の処理と、再生や停止などのAV制御とを行う。通信処理部１６は、AVデータを含むデータリンク層のフレーム（以下では、データリンク層のフレームの例としてイーサネットフレームを用いることとする）を生成して送信するとともに、無線ネットワーク１を介して受信したイーサネットフレームを受信する。著作権保護認証・鍵交換部１７は、著作権保護のために、受信装置３との間で認証や鍵交換処理を行う。

【００１７】

図３は受信装置３の内部構成の一例を示すブロック図である。図３の受信装置３は、インタフェース部２１と、通信処理部２２と、パケット処理部２３と、著作権保護復号化部２４と、RTP処理部２５と、AVデータ再生／蓄積部２６と、著作権保護認証・鍵交換部２７と、AV制御部２８とを有する。

【００１８】

通信処理部２２は、インタフェース部２１にて受信された受信パケットからデータリンク層のフレーム（この例ではイーサネットフレーム）を抽出する。パケット処理部２３は、通信処理部２２で受信されたイーサネットフレームからUDP/IPパケットまたはTCP/IPパケットを抽出する。著作権保護復号化部２４は、著作権保護のために暗号化されて転送されてきたAVデータを復号化する。RTP処理部２５及び著作権保護認証・鍵交換部２７はそれぞれ、RTP処理部１３と著作権保護認証・鍵交換部１７と同様の処理を行う。

【００１９】

著作権保護認証・鍵交換部２７が行う認証・鍵交換処理の少なくとも一部は、

IPパケットを用いてなされてもよいし、IPパケットを用いずに、認証・鍵交換プロトコルを直接イーサネットフレーム上に載せて行ってもよい。図２の送信装置２と図３の受信装置３は、認証・鍵交換プロトコルに利用するデータを直接イーサネットフレーム（または802.11フレーム）上に載せる場合のブロック構成を図示したものである。

【００２０】

本実施形態の送信装置２と受信装置３でやり取りされるデータフォーマットは図４のようなものである。データ本体を表すペイロードｄ１にトランスポート層ヘッダｄ２を付加したUDP/IPパケットに、データリンクヘッダｄ３を付加してデータリンクフレームが生成される。すなわち、AVデータはまずUDP/IPパケットにカプセル化され、さらにUDP/IPパケットは、データリンクフレームにカプセル化される。また、データリンクフレームには物理層ヘッダｄ４が付加される。

【００２１】

なお、データリング層のフレームフォーマットとしては、イーサネットフレームや802.11フレームを用いればよい。802.11フレームの場合、無線ネットワーク１上でのみ使用される制御データ、例えばIEEE802.11無線LANにおけるFCフィールドやDur/IDフィールドなどが含まれるが、図４では簡略化のためにこれらの存在を無視している。

【００２２】

また、トランスポート層のプロトコルとしては、UDP（User Datagram Protocol）やTCP（Transmission Control Protocol）を用い、ネットワーク層のプロトコルとしてはIP（Internet Protocol）を用いればよい。ホームネットワーク１が無線ネットワーク１の場合には、イーサネットフレームにさらに無線レイヤヘッダを付加して無線レイヤフレームが生成され、この無線レイヤフレームが送信装置２から送信される。

【００２３】

図４では、簡略化のために、トレイラの存在を無視している。無線レイヤヘッダには、無線ネットワーク１上でのみ使用される制御データ、例えばIEEE802.11無線LANにおけるFCフィールドやDur/IDフィールドなどが含まれる。

【００２４】

本実施形態では、著作権保護を図る必要のあるAVデータを暗号化して送信する。暗号化するのは、図４のUDP/IPパケットのペイロード部分である。このペイロード部分のより詳細なデータフォーマットは図５のようなものである。AVデータを暗号化したペイロードｄ５に、IETFにて標準化されたAVデータ転送用の転送プロトコルであるRTP（Real-time Transport Protocol）ヘッダｄ６と、UDP/IPヘッダｄ７とを付加し、さらに、RTPヘッダｄ６とペイロードｄ５との間に、著作権保護用制御データｄ８を付加する。この著作権保護用制御データｄ８は、コピー制御情報（以下、CCI）や、AVデータに対して施される暗号化の鍵の値の変化のタイミングを通知するためのビットなどからなる。著作権保護用制御データｄ８は、RTPヘッダの中に含めてもよい。また、著作権保護用制御データｄ８の一部がAVデータと共に暗号化されていてもよい。なお、RTPについては、http://www.ietf.org/rfc/rfc1889.txtを参照されたい。

【００２５】

RTPヘッダｄ6には、ペイロードタイプｄ９が定義されている。本実施形態では、RTPヘッダのペイロードタイプｄ９の値として、ダイナミック・ペイロードタイプの値（＃ｚ）を用いる。ここで、ダイナミック・ペイロードタイプの値を用いるとは、符号化方式ごとに予め定められている割り当て済みのペイロードタイプの値を用いるのではなく、通信ごとに事前にネゴシエーションを行い、利用するペイロードタイプの値を動的に（ダイナミックに）ネゴシエーションした上で決定することを意味する。ネゴシエーションは図２及び図３のAV制御部１８，２８が行う。

【００２６】

これは、従来のRTPと異なり、ペイロードが暗号化されているため、従来のRTPフォーマットとは異なるデータがペイロードに入るという事情と、RTPヘッダとペイロードの間に著作権保護用制御データｄ８が入るという事情による。すなわち従来のRTPのフォーマットと、著作権保護用制御データｄ８が挿入された時のフォーマットが異なるため、RTPパケットを受信した受信装置３は、どちらのフォーマットであるか、あるいは受信したパケットが暗号化されており、復号化が

必要なデータなのか否かを識別する必要がある。

【００２７】

図６は送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第１の実施形態の処理手順を示すシーケンス図である。以下、この図に基づいて、第１の実施形態の暗号化伝送処理を詳しく説明する。なお、著作権保護の仕組みとして、例えば、DTCP（Digital Transmission Content Protection）を想定する。なお、DTCPの詳細については、http://www.dtcp.comを参照されたい。

【００２８】

まず、受信装置３は、送信装置２に対してAVデータの送信を要求する（ステップＳ１）。ここでは、IETFが規定したAVストリーミング機能の遠隔制御用のプロトコルであるRTSP（Real Time Streaming Protocol：RFC2326参照）を用いて、TCP/IP上にてコマンド（プロトコル）のやり取りを行う。なお、RTSP以外に、IEEE1394におけるAV/Cや、UPnP（ユニバーサル・プラグアンドプレイ）プロトコル等によっても、同様の制御を行うことができる。

【００２９】

RTSPでは、(1)AVストリーミング伝送に用いられる符号化方式と、そのビットレート等の各種の属性やパラメータ、(2)使用されるトランスポートプロトコル（TP）の種別（本実施形態の場合はRTP/UDP）、(3)RTPで用いられるペイロードタイプの値（本実施形態の場合、ダイナミック・ペイロードタイプの値を用いる）、(4)通信を行うTCP、またはUDPポート番号の値（本実施形態の場合はTCPを用いる。もちろん、実際にはUDPを用いても良い）、(5)ストリーミングの動作の規定（再生、巻き戻し、停止等）等についてのネゴシエーションを行う。

【００３０】

上記(1)～(5)等で、送信装置２と受信装置３間で合意が得られると、送信装置２は、AVデータを暗号化した後（ステップＳ２）、上記RTSPで合意されたコネクション（本実施形態では、送信装置２のIPアドレス＝ａ、送信ポート番号＝＃ｘ、受信装置３のIPアドレス＝ｂ、受信ポート番号＝＃ｙ）にて、転送プロトコル＝RTP、合意されたダイナミック・ペイロードタイプ（PT）の値（＝＃ｚ）にて、暗号化されたAVデータを含むAVストリームの送信を開始する（ステップＳ３）

。

【００３１】

ステップＳ３で送信されるAVストリームは図５のようなデータフォーマットである。このAVストリームを受信した受信装置３が、例えばAVストリーム中の著作権保護用制御データｄ８により、受信したAVデータに暗号がかけられていることを発見したとする。この場合、受信装置３は送信装置２に対して認証・鍵交換手順を要求し（ステップＳ４）、送信装置２との間で認証・鍵交換処理を行う（ステップＳ５）。認証・鍵交換処理に成功すると、受信装置３は、復号鍵を入手する（ステップＳ６）。

【００３２】

著作権保護用制御データｄ８内の構成は、転送されるAVストリームのトランスポート層のプロトコルにより異なっていてもよい。例えば、トランスポート層のプロトコルがTCPの場合は、暗号化されたAVデータのサイズを示すLengthフィールドを定義してもよい。もちろん、トランスポート層のプロトコルがUDPであっても、Lengthフィールドが定義されていてもかまわない。

【００３３】

この認証・鍵交換の要求と認証・鍵交換処理は、TCP/IPパケット上で行ってもよいし、無線レイヤフレームやイーサネットフレーム上に、認証・鍵交換用のデータを直接載せて行ってもよい。また、この認証・鍵交換手順は、ホームネットワーク１内に留まるべきものであるため、TCP/IPパケット上で行う場合には、TTL（Time To Live）の値をホームネットワーク１内でのみ到達可能な値（たとえば「１」）にした状態で通信を行う等の制限を設けるのが望ましい。

【００３４】

認証・鍵交換は、特定のRTPストリームで転送されるAVストリームに関して行われる。このため、認証・鍵交換を行う前提として、「どのAVストリームに関する認証・鍵交換なのか」についてのネゴシエーションを行う必要がある場合がある。

【００３５】

例えば、受信装置３が、受信したAVストリームが暗号化されていることを認識

し、「このAVストリームについての認証・鍵交換をさせて欲しい」と送信装置２に問い合わせる場合がある。また、送信装置２が、「このAVストリームは、暗号化して受信装置３に対して送出する。このことを、予め，あるいは、AVストリーム転送と同時に、受信装置３に対して通知し、認証・鍵交換のトリガをかけさせる必要がある」と判断し、受信装置３に対して、「このAVストリームは暗号化して送信する。よって、このAVストリームについて認証・鍵交換手順を送信装置２に対して行うべし」という通知を行う場合も考えられる。

【００３６】

もちろん、AVストリーム毎に個々に認証・鍵交換を行うのではなく、「送信装置２と受信装置３の間でやり取りされる、全てのRTPストリームに関して有効とするための認証・鍵交換」を最初に行い、その後は、同送信装置２と受信装置３の間でやり取りされる全てのRTPストリームに関して、上述した認証・鍵交換手順で定められた条件に従って，AVデータの暗号化を行ってもよい。

【００３７】

あるいは、特定のペイロードタイプの値については著作権保護を施すことを、送信装置２と受信装置３の間で予め合意しておき、このようなペイロードタイプの値をもつRTPストリームが受信された場合には、著作権保護が施されているものとしても良い（もちろん、RTSP内にて、設定しているRTPセッションにDTCP著作権保護が施されていることをネゴシエーションする方法も考えられる）。

【００３８】

上述した図６は受信装置３が送信装置２に対して認証・鍵交換のトリガをかける場合の処理手順を示している。受信装置３は、何らかの方法で、受信したAVストリームが暗号化されていることを認識する。例えば、「受信したAVストリームを複号しても、所望のAVストリームを再生できない場合」、あるいは「受信したAVストリームに、図５のような著作権保護用制御データｄ８が付属しており、これを検出して、そのAVストリームが暗号化されていることを認識する場合」、「RTPのペイロードの値としてダイナミックペイロード用の値が用いられており、この値が、データが暗号化されている場合に使われる値であることを認識している場合」等が考えられる。

【００３９】

受信したAVストリームが暗号化されていること、あるいはその可能性があることを認識した受信装置３は、認証・鍵交換要求を送信装置２に対して送出する。この手順もDTCPの手順の一部とすることが可能である。この場合、受信装置３は、その認証・鍵交換要求（あるいは、後続の認証・鍵交換手順パケット）にて、「どのAVストリームについての認証・鍵交換であるか」を明示する。本実施形態では、転送プロトコル種別（RTP）とRTPパケットのペイロードタイプの値（＃ｚ）の値を使う。

【００４０】

ちなみに、送信装置２のIPアドレスとポート番号、及び受信装置３のIPアドレスとポート番号を、その認証・鍵交換要求に明記してもよいし、RTPのSSRCフィールドの値（AVソース毎に一意につけられる識別番号。詳細は、RTPのスペックであるRFC1889を参照のこと）、あるいはIPv6パケット等に含まれる「フローID」の値を用いても良い。

【００４１】

これを受信した送信装置２は、その認証・鍵交換要求（あるいは、認証・鍵交換手続き）が、どのペイロードタイプの値のAVストリームを対象としたものであるかを認識した上で、認証・鍵交換手順を継続する。

【００４２】

認証・鍵交換手順が終了すると、受信装置３は、その認証・鍵交換結果をもとに、その暗号化AVストリームの復号鍵を入手（あるいは、入手するための計算のための初期情報を取得）することができる（ステップＳ６）。

【００４３】

なお、本実施形態において、コンテンツを暗号化するために用いる鍵Ｋｚは、送信装置２と受信装置３の間の認証・鍵交換処理によって生成された鍵Ｋａと、認証・鍵交換が成立した後に送信装置２によってセッション毎にランダムに設定される複数ビット（たとえば64ビット）からなる値Ｋｂ（以後、Ｋｂをシード値とよぶ）を入力とする関数ｆによって生成された値を用いることとする。すなわち、Ｋｚは以下の式によって求められる。

【００４４】

Ｋｚ＝ｆ（Ｋａ，Ｋｂ）

また、ここでは、送信装置２が鍵Ｋａを別な値に設定した時には、必ずシード値Ｋｂを初期化する(ランダムに設定しなおす)こととする。さらに、ＫｂはAVデータ送信中に送信装置２が一定周期ごとに値を常に更新することとする。

【００４５】

従来は、著作権保護用制御データｄ８の中に、Ｋｂの下位１ビットを挿入するフィールドが定義されており、送信装置２はこのフィールドに、コンテンツを暗号化する鍵であるＫｚを計算する際に用いたＫｂの下位１ビットを入れて送信する。

【００４６】

図７は著作権保護用制御データｄ８のデータフォーマットを示す図である。なお、著作権保護用制御データｄ８には、シード値Ｋｂの下位Ｎビットｄ１０と、暗号データパディング長ｄ１１が含まれていてもよい。

【００４７】

AVデータを暗号化する際に用いる暗号アルゴリズムによっては、暗号化のサイズが固定長の倍数単位(例えば8バイトの倍数ごと)に制限される場合がある。例えば、8バイトごとにデータを暗号化するアルゴリズムを用いる場合、14バイトのデータを暗号化するには、元のデータに2バイトのパディングをつける必要がある。この暗号データパディング長ｄ１１は、受信装置の側で何バイトのパディングを挿入したのかを知らせるために用いる。実際の値としては、パディングしたバイトの値でもよいし、パディングする前のデータ長、あるいはそれらの値をコード化した値でもよい。

【００４８】

図８は従来のＫａ，Ｋｂ，Ｋｚの処理方法を示す図である。まず、送信装置２と受信装置３は認証・鍵交換処理を行う（ステップＳ８１）。認証・鍵交換が成功すると、送信装置２と受信装置３は鍵Ｋａを共有することができる（ステップＳ８２，Ｓ８３）。前述のようにAVデータは、この鍵Ｋａとシード値Ｋｂを入力とする関数ｆによって生成された値Ｋｚによって暗号化される。

【００４９】

次に、送信装置２はシード値Ｋｂを初期化（Ｋｂ＝Ａ）する（ステップＳ８４）。受信装置３は送信装置２に対してシード値Ｋｂの問い合わせを行い（ステップＳ８５）、送信装置２はシード値Ａを受信装置３に送信する（ステップＳ８６）。受信装置は、受信されたシード値Ａを設定する（ステップＳ８７）。

【００５０】

送信装置２は、Ｋｚ＝ｆ（Ｋａ，Ａ）にてAVデータを暗号化し（ステップＳ８８）、暗号化したAVデータを送信する（ステップＳ８９）。このとき、AVデータの著作権保護用制御データｄ８の中に現在のシード値Ｋｂの下位１ビットをつけて送信する。

【００５１】

受信装置３はAVデータの著作権保護用制御データｄ８の中に含まれるシード値Ｋｂの下位１ビットの値と、Ｋａとを元にＡＶデータを復号化するための鍵Ｋｚを計算し、ＡＶデータを復号する（ステップＳ９０）。

【００５２】

なお、各ＡＶデータには下位１ビットしか含まれていないため、受信装置３はＫａとＫｂの下位１ビットからだけではＫｚを計算することができない。そこで、認証・鍵交換処理の後に、受信装置３は、上記のステップＳ８５にて、送信装置２によって設定されたＫｂの全ビットの値を問い合わせる処理を行う。

【００５３】

これにより、受信装置３は、最初の一回だけＫｂの値を知り、その後はAVデータの著作権保護用制御データｄ８の中に含まれるＫｂの下位１ビットの変化を観察することで、送信装置２がＫｂを更新したことを検出することができ、更新後のシード値とＫａからコンテンツを復号化する鍵の値を計算することができる。ここで重要なことは、著作権保護用制御データｄ８の中に定義されているＫｂの１ビットはＫｂの値の変化のタイミングを通知することに用いられている点である。

【００５４】

上述したように、送信装置２はAVデータ送信中にＫｂの値を更新する（ステッ

プＳ９１）。なお、更新の方法には、時間によって更新する方法と、送信するAVデータのバイト数ごとに、一定の間隔で（たとえば1づつ）更新する方法がある。ここでは説明を簡略化するために、一定バイト数ごとにシードの値を１づつ増加させることとする。

【００５５】

図８では、送信装置２がＫｂの値をＡからＡ＋１に更新したことを示している。Ｋｂの更新によってコンテンツの暗号化に用いる鍵Ｋｚの再計算を行う。具体的にはＫａとＡ＋１から関数ｆを用いて計算した値Ｋｚ´を求める。このＫｚ´を用いてコンテンツを暗号化して送信する（ステップＳ９２，Ｓ９３）。なお、Ｋｚ´によって暗号化されたAVデータの著作権保護用制御データｄ８の中にはＡ＋１の下位１ビットを含める。

【００５６】

このAVデータを受信した受信装置３はAVデータの著作権保護用制御データｄ８の中に含まれるＫｂの下位１ビットの値から、ＫｂがＡからＡ＋１に変化したことを知ることができ（ステップＳ９４）、ＫａとＡ＋１から関数ｆを用いてコンテンツを復号する鍵Ｋｚ´の値を計算することができる。これにより、受信したAVデータを正しく復号することができる（ステップＳ９５）。

【００５７】

なお、シード値の問い合わせや応答に用いるメッセージは認証・鍵交換で用いるメッセージと同様に、IPパケットを用いてなされてもよいし、IPパケットを用いずに、認証・鍵交換プロトコルに利用するデータを直接802.11フレーム(またはイーサネットフレーム)上に載せて行ってもよい。

【００５８】

図９は送信装置２のコンテンツ鍵更新の検出処理手順を示すシーケンス図である。以下、図９を参照しながら、本実施形態の特徴である著作権保護用制御データｄ８の中に含めるシード値Ｋｂを、下位１ビットではなく下位複数ビットに設定することの効果について説明する。ここでは、シード値Ｋｂが一定周期で更新され、現在の値がＢになっているものとする。

【００５９】

まず、送信装置２は、暗号鍵Ｋｚｌ＝ｆ（Ｋａ，Ｂ）でAVデータを暗号化して（ステップＳ１０１）、受信装置３に送信する（ステップＳ１０２）。受信装置３は、このAVデータを復号鍵Ｋｚｌ＝ｆ（Ｋａ，Ｂ）で復号する（ステップＳ１０３）。

【００６０】

ここで、送信装置２がAVデータの出力を停止したり、再起動したりする等の理由により、受信装置３と共有していたＫａを破棄し（ステップＳ１０４）、新しい値Ｋａ´に更新したとする（ステップＳ１０５）。これと同時にシード値も初期化され、Ｂとは異なる値Ｃに再設定される（ステップＳ１０６）。

【００６１】

RTPにおいては、下位レイヤにコネクションレス型のプロトコルUDPを用いることが一般的である。コネクションレス型のプロトコルでは、受信装置と送信装置は互いに状態を保持しないため、仮に送信装置２がセッションを破棄したとしても、受信装置３はこれを検出することができない。

【００６２】

従って、従来方法においては仮に送信装置２が再起動して鍵の値をＫａ´に更新したとしても、そのことを受信装置３が知る手段がない。またコネクションレス型のプロトコルを使った場合、送信装置と受信装置の間の伝送系路上でパケットが喪失した場合や、受信装置がパケットを受信できなかった場合には、このパケットロスが行ったことを知る手段がない。しかし、著作権保護用制御データｄ８の中に含めるシード値Ｋｂを、下位複数ビットに設定することで、Ｋａの変化を受信装置３で検出したり、パケットロスが起こったりしたことを検出することができる。その理由を以下に示す。

【００６３】

まず、シード値の変化を検出する手段について述べる。受信装置３と共有していたＫａを送信装置２が破棄し、新しい値Ｋａ´に更新したとする。送信装置２は、再設定された鍵Ｋａ´とシード値Ｃを用いてコンテンツを暗号化する鍵Ｋｚ２を求め、Ｋｚ２によってAVデータを暗号化して送信する（ステップＳ１０７，Ｓ１０８）。このAVデータを受信した受信装置３は、著作権保護用制御データｄ

８の中に含めるシード値の下位Ｎビットがｃであり、これまで受信してきた値ＢまたはＢを更新した値Ｂ＋１ではないことが分かる。

【００６４】

Ｋｂのビット長が十分に長ければ、初期化によってランダムに設定された値（Ｃ）と、以前に利用していた値（ＢないしＢ＋１）が一致する確率は低く、受信装置は期待していた値ＢまたはＢ＋１ではないAVデータを受信した場合、送信装置２は鍵Ｋａを更新したことを暗号処理の中で検出することができる（ステップＳ１０９）。

【００６５】

次に、送信装置と受信装置の間の通信経路上でパケットロスが発生したことを検出する方法について述べる。

【００６６】

図１０にAVデータの中の著作権保護用制御データｄ８の中に含めるシード値を下位１ビットにした場合の処理手順の一例を示す。送信装置２と受信装置３がシード値を共有するまでは図８のステップＳ８６と同様の手順でよい。ここで仮に共有したシード値をＥとする（ステップＳ１２１）。また、Ｅの最下位ビットは０であるとする。送信装置２は前述したルールにより、一定周期ごとにシード値を更新する（ステップＳ１２８）。ここでは、ＥからＥ＋１、Ｅ＋２、Ｅ＋３と更新することとする。すなわち、Ｅ＋１の最下位ビットは１であり、Ｅ＋２の最下位ビットは０、Ｅ＋３は１である。

【００６７】

AVデータに付属する著作権保護用制御データｄ８の中に含めるシード値が下位１ビットである場合、送信装置２がシード値Ｅで暗号化したAVデータについては、受信装置３は、Ｅの最下位ビットである０を受信し、送信装置２のシード値がＥ＋１，Ｅ＋２、Ｅ＋３と更新される度に１、０、１の順で受信し、Ｅ＋１、Ｅ＋２、Ｅ＋３のシード値で受信したAVデータを復号化する（ステップＳ１２４，Ｓ１２７，Ｓ１３２）。

【００６８】

次に、パケットロスが発生した場合の処理手順を図１１に示す。シード値Ｅに

てAVデータが送受信されるまでは図１２と同様の手順でよい。ここで仮に受信装置３はシード値をＥ＋１としたデータすべての受信に失敗したとする（ステップＳ１４５，Ｓ１４６）。

【００６９】

コネクションレスのプロトコルでは、損失したデータの再送は行わないため、受信装置３はＥ＋１のデータの受信に失敗したことを知ることはできない。すなわち、受信装置３は、シード値がＥの最下位ビット０を受信した後、シード値Ｅ＋２の最下位ビット０を受信するため、シード値の更新は行われない。このため、送信装置２はシード値Ｅ＋２にてAVデータを暗号化しているにもかかわらず、受信装置３はシード値Ｅにて受信したAVデータを復号化するため、正しく復号化することができない（ステップＳ１５０）。

【００７０】

一方、著作権保護用制御データｄ８の中に含めるシード値を下位複数ビットである場合の処理手順を図１２に示す。この図では説明を簡略化するために、シード値のビット数を３ビットとしてある。この場合、受信装置３は仮にシード値Ｅ＋１で暗号化されたデータの受信に失敗したとしても、Ｅ＋２で暗号化されたデータに含まれるシード値の値を確認することで（ステップＳ１６９）、シード値が更新されたことを検出することができ、AVデータを正しく復号することができる（ステップＳ１７０）。

【００７１】

同様の目的を達成するには、シード値のすべてのビットを著作権保護用制御データｄ８に含めたり、コンテンツ暗号鍵の番号を新たに定義したりすることでも可能である。しかし、すべてのビットを転送する場合と比較して、シード値の下位Ｎビットを転送することで、ヘッダの大きさを抑えることができ、AVデータを効率よく転送することができる。

【００７２】

図１３は、著作権保護用制御データｄ８の中に含めるシード値Ｋｂを、下位複数ビットに設定する場合の受信装置３の内部構成を示すブロック図である。図３との違いは、受信したAVデータの著作権保護用制御データｄ８の中に含まれるシ

ード値の値が、以前受信したシード値と同じか、あるいはそのシード値から予測可能な値（たとえば１大きい値）であるか否かを判定し、もし期待された値でなかった場合には認証・鍵交換をやり直すことを著作権保護認証・鍵交換処理部に通知する機能をもつシード値更新検出部２９を持つ点である。

【００７３】

このように、第１の実施形態では、著作権保護の必要なAVデータを暗号化したペイロードに、プロトコル種別（例えばRTP）と、このプロトコルが使用するペイロードタイプの値と、を付加したAVストリームを送信装置２から受信装置３に送信するため、このAVストリームを受信した受信装置３は、AVデータが暗号化されていることを容易に検出でき、かつ認証・鍵交換が必要なデータを容易に識別できる。これにより、著作権保護を図りつつ、AVデータを簡易かつ迅速に受信及び再生できる。

【００７４】

また、復号鍵を生成するためのシード値をそのまま受信装置３に送信するのではなく、シード値の一部のビットのみを受信装置３に送信することにより、AVデータのデータ量を抑制できるとともに、セキュリティ性も向上できる。

【００７５】

（第２の実施形態）

第２の実施形態は、AVデータを暗号化して送信したことを送信装置２から受信装置３に通知するものである。

【００７６】

第２の実施形態の送信装置２及び受信装置３はそれぞれ図２及び図３と同様に構成されているが、AVデータの暗号化伝送処理の一部が第１の実施形態と異なっている。

【００７７】

図１４は送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第２の実施形態の処理手順を示すシーケンス図である。第２の実施形態では、送信装置２が受信装置３に暗号化されたAVデータを含むAVストリームを送信した後に（ステップＳ１３）、AVデータが暗号化されていることを通知するためのAVストリーム

暗号化通知を送信装置２が受信装置３に送信する（ステップＳ１４）。この通知は、送信装置２が送信したAVストリーム（ペイロードタイプ＝＃ｚ）がDTCP等のプロトコルに従って暗号化され、これを受信装置３が復号するには、送信装置２との間で認証・鍵交換を行う必要があることを受信装置３に知らせるものである。この通知は、IPパケットを用いて行ってもよいし、無線レイヤパケット、もしくはイーサネットフレームを用いて行ってもよい。またはコンテンツ指定の応答メッセージとして、「コンテンツを暗号化して送信する」ことをHTTPのレスポンスメッセージの中に含めてもよいし、SDP（Session Description Protocol：RFC2327参照）を拡張した形式で送信してもよい。

【００７８】

図１５は、受信装置３が送信装置２に対して所望のAVデータを指定し、その指定に対する応答として、当該AVデータが暗号化されていることを通知する場合の処理手順を示すシーケンス図である。

【００７９】

まず、受信装置３は、AV制御コマンドを送信装置２に対して送信した後（ステップＳ２１）、AVデータのコンテンツを指定する（ステップＳ２２）。このコンテンツの指定方法としては、例えばHTTP等の公知の手法を用いればよい。

【００８０】

送信装置２は、指定されたコンテンツが著作権を保護すべきコンテンツであることをコンテンツの付加情報等から認識し（ステップＳ２３）、AVデータを暗号化して送信した後（ステップＳ２４，Ｓ２５）、AVストリーム暗号化通知をHTTPのレスポンスメッセージまたはSDPにて送信する（ステップＳ２６）。これにより、受信装置は、送信装置２との間で認証・鍵交換を行う必要があることを知る。

【００８１】

受信したAVストリーム（ペイロードタイプ＃ｚのAVストリーム）が暗号化されることを認識した受信装置３は、認証・鍵交換要求を送信装置２に対して送信し（ステップＳ２７）、送信装置２と受信装置３との間で認証・鍵交換処理を行う（ステップＳ２８）。

【００８２】

なお、図１４及び図１５では、ペイロードタイプの値として特定の値（＃ｚ）を通知する形の例を示したが、著作権保護を施すペイロードタイプの２種類以上の値からなる範囲（例えば＃ｚ１～＃ｚ２の範囲の値）を通知してもよい。

【００８３】

このように、第２の実施形態では、AVストリーム中のAVデータが暗号化されていることを送信装置２が受信装置３に通知するため、受信装置３は、受信したAVストリーム中のAVデータが暗号化されているか否かを自分自身で調べる必要がなくなる。したがって、受信装置３の処理を軽減できるとともに、認証・鍵交換処理が完了するまでの時間を短縮できる。

【００８４】

（第３の実施形態）

第３の実施形態は、AVデータを送信する前に、著作権保護のための認証・鍵交換を行うものである。

【００８５】

第３の実施形態の送信装置２及び受信装置３はそれぞれ図２及び図３と同様に構成されているが、AVデータの暗号化伝送処理の一部が第１及び第２の実施形態と異なっている。

【００８６】

図１６は送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第３の実施形態の処理手順を示すシーケンス図である。まず、受信装置３は、送信装置２に対して、IPパケットまたはイーサネットフレームにて、認証・鍵交換を要求する（ステップＳ３１）。そして、送信装置２と受信装置３との間で、認証・鍵交換処理を行い（ステップＳ３２）、認証・鍵交換処理に成功すると、受信装置３は復号鍵を取得する（ステップＳ３３）。

【００８７】

この認証・鍵交換の間に、「RTPのペイロードタイプの値が＃ｚ１～＃ｚ２の間の場合には、そのRTPセッションのデータはDTCPにて著作権保護のための暗号化が施されており、更にRTPヘッダとRTPペイロードの間にDTCP用の制御データが

挿入される」ということを、認証・鍵交換の段階で送信装置２と受信装置３の間で共有する。

【００８８】

その後、受信装置３は、送信装置２に対してAVデータの送信を要求し（ステップＳ３４）、これを受けて送信装置２はAVデータを暗号化し（ステップＳ３５）、図４のフォーマットのIPパケットまたはイーサネットフレームを受信装置３に向けて送信する（ステップＳ３６）。図１６の例では、ペイロードタイプの値の範囲を＃ｚ１～＃ｚ２にして、暗号化したAVデータを伝送している。

【００８９】

受信装置３は、ペイロードタイプの値を参照することで、そのAVストリームがDTCPにて暗号化されていることを認識でき、適切な復号化手順を経て、AVストリームの再生を行うことができる。

【００９０】

この他にも、認証・鍵交換手順に、対象とするペイロードタイプの値を含めておき、そのコマンドが要求する何らかの手順（例えば、最新の鍵の値を問い合わせる等）の対象が、特定のペイロードタイプのＡＶストリームについてのものであることを通知する手順を加えてもよい。

【００９１】

このように、第３の実施形態では、受信装置３から認証・鍵交換要求を行って、認証・鍵交換処理に成功した場合に限り、送信装置２から受信装置３に対して、暗号化したAVデータを含むAVストリームを送信するため、無駄にAVストリームを送信しなくて済み、通信効率の向上が図れるとともに、セキュリティ性も向上する。

【００９２】

（第４の実施形態）

第４の実施形態では、送信装置２がAVデータを送信するに先立ち、受信装置３とAVデータの暗号フレームサイズの決定を行うものである。

【００９３】

第４の実施形態における送信装置２はAVデータをある一定のサイズに分割し、

暗号化して受信装置３に送信する。なお、分割されたこの1つの暗号フレームは、単一の暗号ブロックで構成されていてもよいし、暗号ブロックをチェーンさせた暗号ブロックチェーン（CBC：Cipher Block Chain）であってもよい。暗号フレームサイズとは、単一の暗号ブロックの場合はブロック長を指し、暗号ブロックチェーンの場合はチェーンさせた時のサイズを指す。

【００９４】

送信装置２と受信装置３がAVデータの暗号フレームサイズを合意する方法には、(1)送信装置２と受信装置３があらかじめ合意したサイズとする方法、(2)送信装置２から受信装置３へ通知する方法、(3)受信装置３から送信装置２へサイズを通知する方法、(4)(1)から(3)の方法を組み合わせた方法、など種々の方法がある。

【００９５】

(1)の場合、各ベンダーは予め文書等で定められた暗号フレームサイズに従って送信装置２はデータを暗号化し、受信装置は復号化する方法である。

【００９６】

(2)は、送信装置がAVデータ送信に先立ち、受信装置へ暗号フレームサイズを指定する方法である。

【００９７】

図１７は送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第３の実施形態の処理手順を示すシーケンス図である。まず、受信装置３は、送信装置２に対してAVデータの送信を要求する（ステップＳ４１）。これを受けて、送信装置２はAVデータの暗号化を行う（ステップＳ４２）。

【００９８】

次に、送信装置２は、AVデータが暗号化されていることを通知するためのAVストリーム暗号化通知を受信装置３に送信する（ステップＳ４３）。ここまでは第２の実施形態と同様である。

【００９９】

送信装置２は、AVストリームを一定単位で暗号化するサイズを通知するためのAVストリーム暗号フレームサイズ通知を受信装置３に送信する（ステップＳ４４

）。もちろん、AVストリーム暗号化通知とAVストリーム暗号フレームサイズ通知は同一のパケットで送ってもよいし、別々なパケットとして順番を入れ替えて送ってもよい。

【０１００】

なお、図１７では、第２の実施形態の処理手順の一部に、AVストリーム暗号フレームサイズ通知を含める例を説明したが、この通知は第２の実施形態に限ったものではなく、送信装置２が受信装置３に対してAVデータを送信する前であれば、第１の実施形態や第３の実施形態においても適用可能である。

【０１０１】

(3)は、受信装置３から送信装置２へ処理可能な暗号フレームサイズを通知する方法である。

【０１０２】

この方法における受信装置３のブロック構成は図１８のようになる。図１８では、第１～第３の実施形態における受信装置３の内部構成を示した図３と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。

【０１０３】

図３との違いは、著作権保護認証・鍵交換部２７の中に暗号フレームサイズ通知送信部３０を備えている点と、著作権保護認証・鍵交換部２７にて生成された情報がパケット処理部２３によってトランスポート層のパケットにカプセル化される点である。

【０１０４】

暗号フレームサイズ通知送信部３０は、著作権保護復号化部２４がAVデータを復号する際に処理可能な暗号フレームサイズに関する情報を有しており、このサイズを著作権保護認証・鍵交換処理部２７のコマンドの一部として定義しておく。

【０１０５】

なお、図３では、著作権保護認証・鍵交換部２７にて生成された情報は、インターフェース部２１によって無線レイヤのフレームにカプセル化されて送信されたが、図１８ではパケット処理部２３によってTCP/IPパケット化して送信する。

もちろん、図３に示した方法と同様に、無線レイヤのフレームにカプセル化して送信するようにしてもよいし、通信処理部２２を利用して直接データリンク層のフレームにカプセル化して送信するようにしてもよい。

【０１０６】

また、図１８では著作権保護復号化部２４が処理可能な暗号フレームサイズに関する情報を、暗号フレームサイズ通知送信部３０が有している場合について示したが、(a)著作権保護復号化部２４が可変の暗号フレームサイズを処理可能な場合、(b)著作権保護復号化部２４に処理可能な暗号フレームサイズに関する情報が保存されている場合については、暗号フレームサイズ通知送信部３０が著作権保護復号化部２４に問い合わせるようにしてもよい。その場合の内部構成は図１９のようになる。

【０１０７】

図２０は(3)の方法における送信装置２の構成を示すブロック図である。図２０では、第１から第３の実施形態における送信装置２の内部構成を示した図２と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。図２との違いは、著作権保護認証・鍵交換部１７の中に暗号フレームサイズ通知受信部１９を備えている点と、著作権保護認証・鍵交換部１７にて生成された情報がパケット処理部１５によってトランスポート層のパケットにカプセル化される点である。暗号フレームサイズ通知受信部１９は、著作権保護認証・鍵交換処理部のコマンドの一部として定義された、暗号フレームサイズを通知するコマンドを受信すると、暗号フレームサイズに関する情報を抽出する機能を持つ。さらに、抽出した暗号フレームサイズを著作権保護暗号化部１４に通知する機能を持つ。

【０１０８】

著作権保護暗号化部１４は、受信装置３から指定された暗号フレームサイズに従って、AVデータを暗号化する。

【０１０９】

図２１は当該方法における暗号フレームサイズの指定方法の処理手順を示すシーケンス図である。認証・鍵交換手順までの手順は第２の実施形態と同様の方法

でよい。認証・鍵交換が成立し、送信装置２と受信装置３とでコンテンツの復号化に用いる鍵が共有すると、受信装置３は送信装置２に対して、AVストリーム暗号フレームサイズ通知を行う。受信装置２は、通知されたサイズに従って、AVデータを暗号化し受信装置に対して送信する。

【０１１０】

なお、送信装置２の著作権保護暗号化部１４が処理できないサイズを受信装置３から通知された場合には、逆に送信装置２が受信装置３に対して、暗号化サイズを指定するようなメッセージを送信する機能を持っていてもよい。その場合の送信装置２および受信装置３の内部構成をそれぞれ図２２と図２３に示される。

【０１１１】

送信装置２が通知されたサイズの値で処理できない場合とは、たとえば送信装置に指定されたサイズでAVデータを暗号化する機能がない場合や、すでに送信装置がマルチキャストにてAVデータの送信を行っており、途中で暗号フレームサイズを変更することができない場合などを指す。

【０１１２】

マルチキャスト通信の場合、1台目で送信装置と受信装置の暗号フレームサイズが決定されると、マルチキャスト通信の途中で2台目以降が参加して暗号フレームサイズの指定要求を行ったとしても通信途中でサイズを変更することができない。この場合、送信装置が暗号フレームサイズ(マルチキャスト通信の場合、現在利用している暗号フレームサイズの値)を受信装置に指定することになる。

【０１１３】

なお、マルチキャスト通信の場合には、上述した方法以外にも、送信装置２と受信装置３があらかじめ合意したマルチキャスト用の暗号フレームサイズとする方法、またはネゴシエーションによって送信装置２と受信装置３があらかじめ合意したマルチキャスト用のサイズとする方法といった、(1)もしくは(1)と(2)、(3)を組み合わせた方法をとることができる。

【０１１４】

図２４はマルチキャスト通信において、送信装置２と受信装置３があらかじめ合意したマルチキャスト用の暗号フレームサイズにてAVデータを暗号化する処理

手順を示すシーケンス図である。送信装置２がAVデータをマルチキャストにて送信する場合、あらかじめ定められたマルチキャスト用の暗号フレームサイズに従ってAVデータを暗号化して送信する。受信装置３は、マルチキャストにて受信したAVデータをあらかじめ定められたマルチキャスト用の暗号フレームサイズに従って復号する。

【０１１５】

このように、マルチキャスト通信以外の場合とマルチキャスト通信の場合とで、暗号フレームサイズを分ける。これにより、送信装置２がAVデータを送信途中に追加的に参加してきた受信装置に対して、通信途中で暗号フレームサイズを変更する必要がなく、またAVデータが受信できないような受信装置３の開発を未然に防ぐことができる。もちろん、マルチキャスト専用の暗号フレームサイズをあらかじめ複数定義しておき、その中から(2)または(3)で示したネゴシエーションの方法により送信装置２と受信装置３が選択するような方法になっていてもよい。

【０１１６】

このマルチキャスト専用の暗号フレームサイズを定義する方法における受信装置３のブロック構成は図２５のようになる。図１８との違いは、マルチキャスト用暗号フレームサイズ通知部３１を備えている点である。マルチキャストにてAVデータを受信した場合には、マルチキャスト用暗号フレームサイズ通知部３１は、マルチキャスト用の暗号フレームサイズを著作権保護復号化部２４に通知する機能を持つ。

【０１１７】

著作権保護復号化部２４は、受信装置３から受信したAVデータをマルチキャスト用暗号フレームサイズ通知部３１によって通知された暗号フレームサイズに従って復号化する。

【０１１８】

また送信装置２のブロック構成は図２６のようになる。図２０との違いは、マルチキャスト用暗号フレームサイズ通知部２０を備えている点である。マルチキャストにてAVデータを送信する場合には、マルチキャスト用暗号フレームサイズ

通知部２０は、マルチキャスト用の暗号フレームサイズを著作権保護暗号化部１４に通知する機能を持つ。著作権保護暗号化部１４は、AVデータを通知された暗号フレームサイズに従って暗号化する。

【０１１９】

図２７はこれら暗号フレームサイズのネゴシエーションに使うデータフォーマットの一例を示す図である。サイズ指定要求パケットは、受信装置３が送信装置２に処理可能な暗号フレームサイズの指定を行う際に用いられ、IPヘッダｄ２１と、TCPヘッダｄ２２と、著作権保護用共通制御ヘッダｄ２３と、暗号フレームサイズ要求ｄ２４と、サイズの値ｄ２５とを有する。

【０１２０】

サイズ指定応答パケットは、サイズ指定要求パケットを受信した送信装置２が指定されたサイズでの送信を許可するか、拒絶する際に用いられ、IPヘッダｄ３１と、TCPヘッダｄ３２と、著作権保護用共通制御ヘッダｄ３３と、暗号フレームサイズ応答ｄ３４と、サイズの値ｄ３５とを有する。

【０１２１】

サイズ指定応答パケットのサイズの値は、拒絶する際には必須となるが、許可する際には値を入れても入れなくても、どちらでもよい。

【０１２２】

また、ここでは、第２の実施形態の処理手順の一部としてAVストリーム暗号フレームサイズ通知を含めたが、この通知は第２の実施形態に限ったものではなく、受信装置３が送信装置２から復号化可能な状態でAVデータを受信する前であれば第１の実施形態や第３の実施形態においても適用可能である。ここで復号可能な状態とは、送信装置２と受信装置３の間で認証・鍵交換が成立し、受信したAVストリームを復号化できる状態にあることを指す。

【０１２３】

このように、第４の実施形態によれば、受信装置３から送信装置２に処理可能な暗号フレームサイズを通知するため、受信装置３は用途に合わせた暗号フレームサイズを処理可能な暗号処理モジュールを実装することができ、機器の製造コストをおさえることができる。

【０１２４】

例えば、携帯型オーディオ機器の場合には、AVデータのデータサイズも小さく、また送信レートも低い。このためセキュリティ上の観点から暗号フレームサイズを小さくすることが望ましい。一方、有線接続される高解像度の画像が受信可能なテレビなどは、AVデータのサイズも大きく送信レートも高い。このため、暗号フレームサイズを大きくすることが望ましい。なぜならば暗号フレームサイズが小さい場合、大量のデータを小さなサイズに区切って暗号・復号処理を施さなければならず、そのための高速の処理モジュールを備える必要があるため、機器のコストが増大するためである。また、下位のネットワークレイヤによっても適切な暗号フレームサイズは異なる。例えば、トランスポート層のプロトコルとしてUDPを用いるとする。データリンク層の最大パケットサイズを越えたUDPパケットを送信しようとすると、1つのUDPパケットは複数のデータリンクフレームに分割される。UDPは再送処理機構を備えていないため、この時分割されたデータリンクフレームのうち、1つのフレームでも欠落した場合には、UDPパケット全体が損失することになる。この時の暗号フレームサイズを大きく決定した場合、1つのUDPフレームが欠落した場合、その暗号フレームサイズのデータを復号化することができなくなってしまう。このように転送効率を考慮して、暗号フレームサイズをデータリンクフレームのサイズにあわせて送信することがある。

【０１２５】

このように機器の性能やAVデータの特性、ネットワークの特性によって適切な暗号フレームサイズは異なるため、ネゴシエーション処理を行い、その都度適切な暗号化サイズを決定することが望ましい。

【０１２６】

上述した図６～図８の処理は、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。ソフトウェアで実現する場合には、図６～図８の処理の少なくとも一部を実現するプログラムをフロッピーディスクやＣＤ－ＲＯＭ等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【０１２７】

また、図６～図８の処理の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【０１２８】

上述した実施形態で説明した送信装置２及び受信装置３は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、送信装置２及び受信装置３の少なくとも一部の機能を実現するプログラムをフロッピーディスクやＣＤ－ＲＯＭ等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【０１２９】

また、送信装置２及び受信装置３の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【０１３０】

【発明の効果】

以上詳細に説明したように、本発明によれば、ネゴシエーションしたペイロードタイプの値を含むパケットを送信装置と受信装置との間で送受するため、そのパケットに含まれる電子データが著作権保護を図る必要があるか否かを識別でき、著作権保護を図りつつ、電子データを簡易かつ迅速に送受信できる。

【図面の簡単な説明】

【図１】

本発明の一実施形態である送信装置と受信装置とを備えたAV通信システムの概

略構成を示すブロック図。

【図２】

送信装置の内部構成の一例を示すブロック図。

【図３】

受信装置の内部構成の一例を示すブロック図。

【図４】

送信装置と受信装置でやり取りされるデータフォーマットを示す図。

【図５】

図４のより詳細なデータフォーマットを示す図。

【図６】

送信装置と受信装置が行うAVデータの暗号化伝送処理の第１の実施形態の処理手順を示すシーケンス図。

【図７】

著作権保護用制御データｄ８のデータフォーマットを示す図。

【図８】

従来のＫａ，Ｋｂ，Ｋｚの処理方法を示す図。

【図９】

送信装置のコンテンツ鍵更新の検出処理手順を示すシーケンス図。

【図１０】

シード値を下位１ビットにした場合の処理手順の一例を示すフローチャート。

【図１１】

パケットロスが発生した場合の処理手順の一例を示すフローチャート。

【図１２】

シード値が複数ビットの場合の処理手順の一例を示すフローチャート。

【図１３】

著作権保護用制御データｄ８の中に含めるシード値Ｋｂを、下位複数ビットに設定する場合の受信装置３の内部構成を示すブロック図。

【図１４】

送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第２の実施形態の

処理手順を示すシーケンス図。

【図１５】

受信装置３が送信装置２に対して所望のAVデータを指定し、その指定に対する応答として、当該AVデータが暗号化されていることを通知する場合の処理手順を示すシーケンス図。

【図１６】

送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第３の実施形態の処理手順を示すシーケンス図。

【図１７】

送信装置２と受信装置３が行うAVデータの暗号化伝送処理の第３の実施形態の処理手順を示すシーケンス図。

【図１８】

暗号フレームサイズ通知送信部を有する受信装置の内部構成を示すブロック図。

【図１９】

図１８の変形例を示すブロック図。

【図２０】

暗号フレームサイズ通知受信部を有する送信装置の内部構成を示すブロック図。

【図２１】

暗号フレームサイズの指定方法の処理手順を示すシーケンス図。

【図２２】

暗号フレームサイズの指定を行う受信装置の内部構成を示すブロック図。

【図２３】

暗号フレームサイズの指定を受ける送信装置の内部構成を示すブロック図。

【図２４】

マルチキャスト通信において、送信装置と受信装置があらかじめ合意したマルチキャスト用の暗号フレームサイズにてAVデータを暗号化する処理手順を示すシーケンス図。

【図２５】

マルチキャスト専用の暗号フレームサイズを定義する場合の受信装置のブロック図。

【図２６】

マルチキャスト専用の暗号フレームサイズを定義する場合の送信装置のブロック図。

【図２７】

サイズ指定要求パケットとサイズ指定応答パケットのデータフォーマットを示す図。

【符号の説明】

１　ホームネットワーク

２　送信装置

３　受信装置

１１　インタフェース部

１２　AVデータ生成／蓄積部

１３　RTP処理部

１４　著作権保護暗号化部１４

１５　TCP/IPパケット送受信部

１６　イーサネットフレーム送受信部

１７　著作権保護認証・鍵交換部

２１　インタフェース部

２２　イーサネットフレーム送受信部

２３　TCP/IPパケット送受信部

２４　著作権保護復号化部

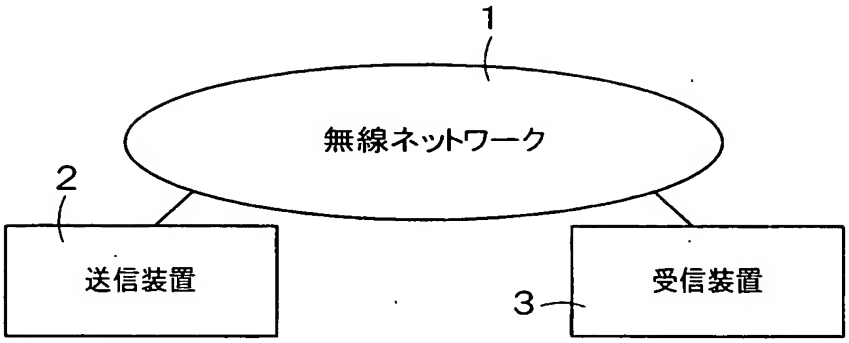
２５　RTP処理部

２６　AVデータ再生／蓄積部

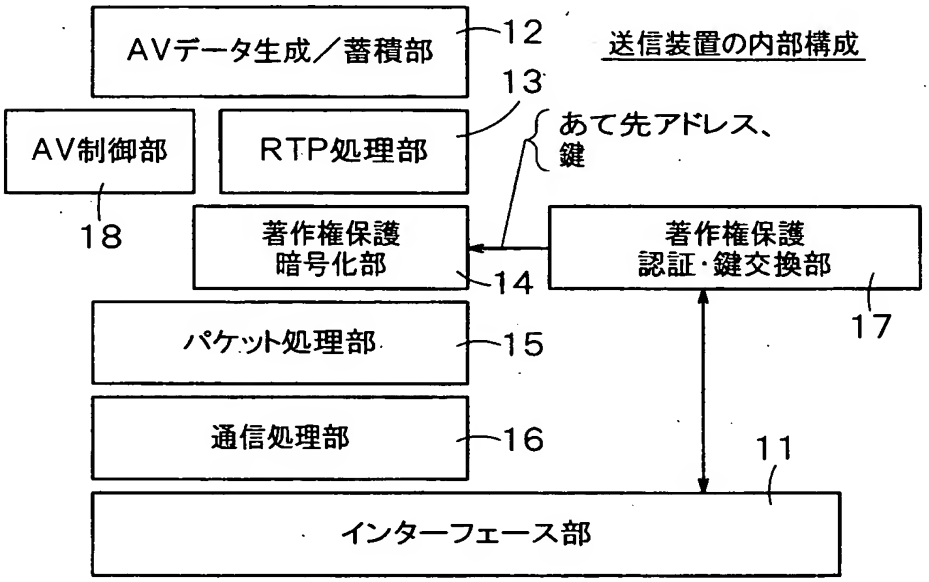
２７　著作権保護認証・鍵交換部

【書類名】　図面

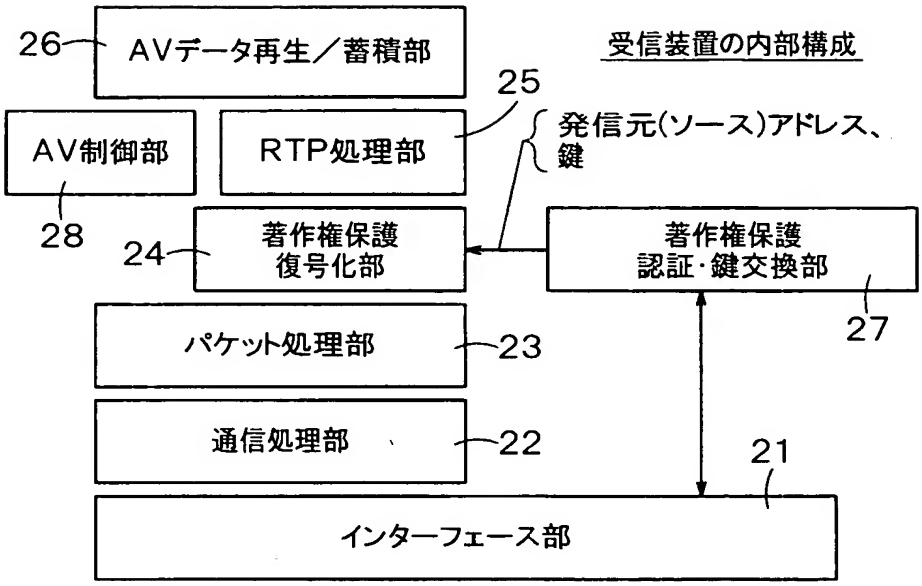
【図１】


1
無線ネットワーク
2
送信装置
3
受信装置

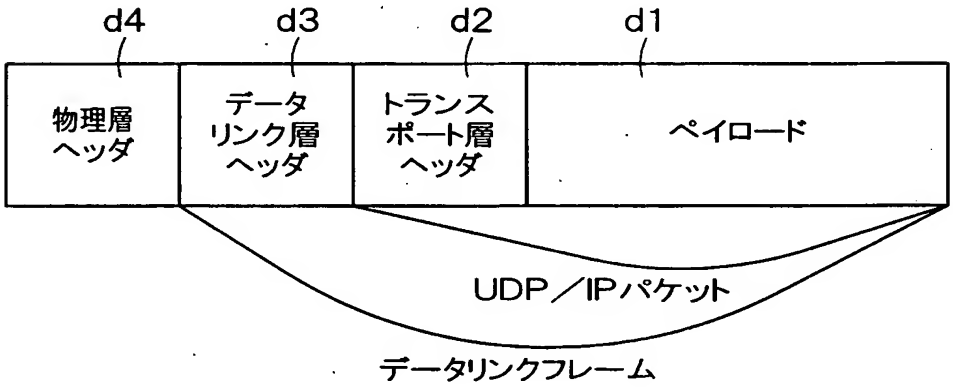
【図２】


AVデータ生成／蓄積部
12
送信装置の内部構成
13
AV制御部
RTP処理部
あて先アドレス、
鍵
18
著作権保護
暗号化部
14
著作権保護
認証・鍵交換部
17
パケット処理部
15
通信処理部
16
11
インターフェース部

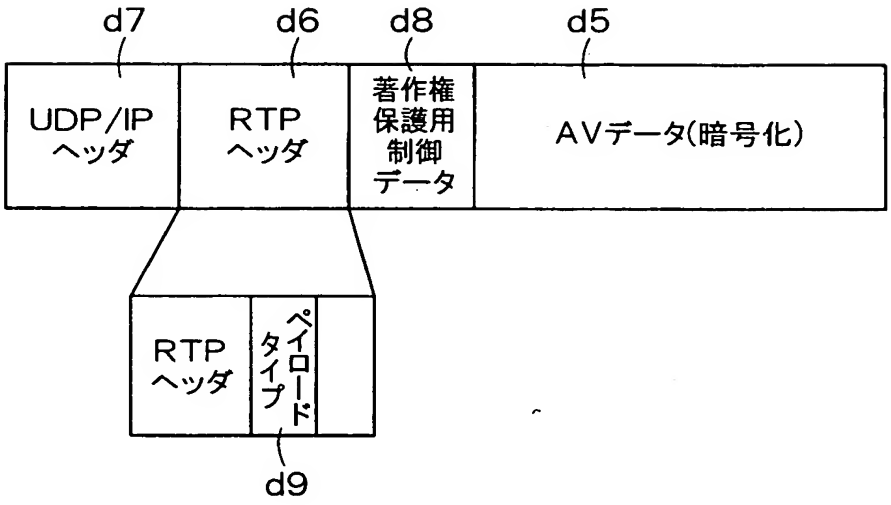
【図３】


受信装置の内部構成
26
AVデータ再生／蓄積部
25
発信元(ソース)アドレス、
鍵
AV制御部
RTP処理部
28
24
著作権保護
復号化部
著作権保護
認証･鍵交換部
27
パケット処理部
23
通信処理部
22
21
インターフェース部

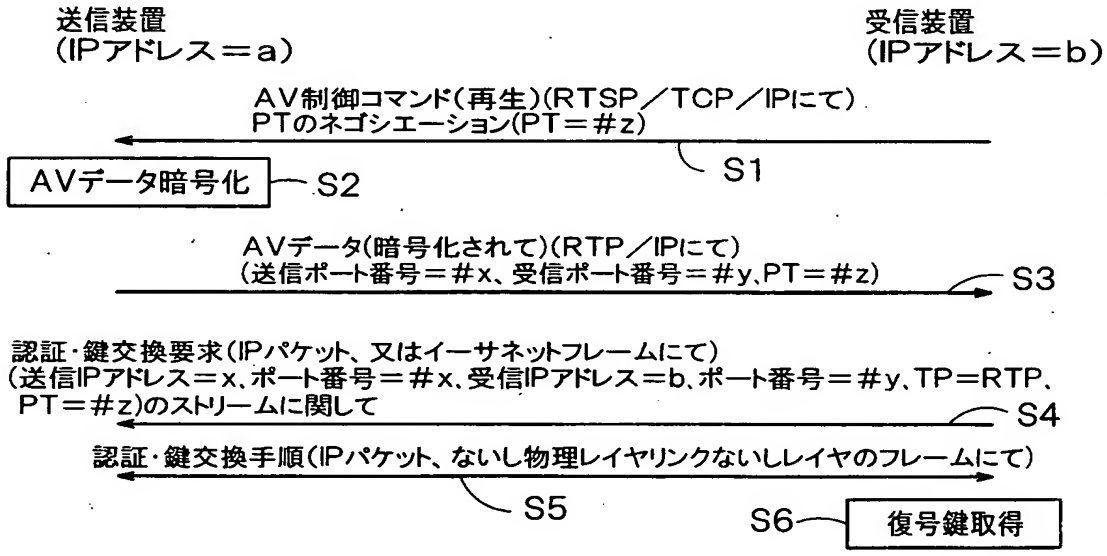
【図４】


d4
d3
d2
d1
物理層
ヘッダ
データ
リンク層
ヘッダ
トランス
ポート層
ヘッダ
ペイロード
UDP／IPパケット
データリンクフレーム

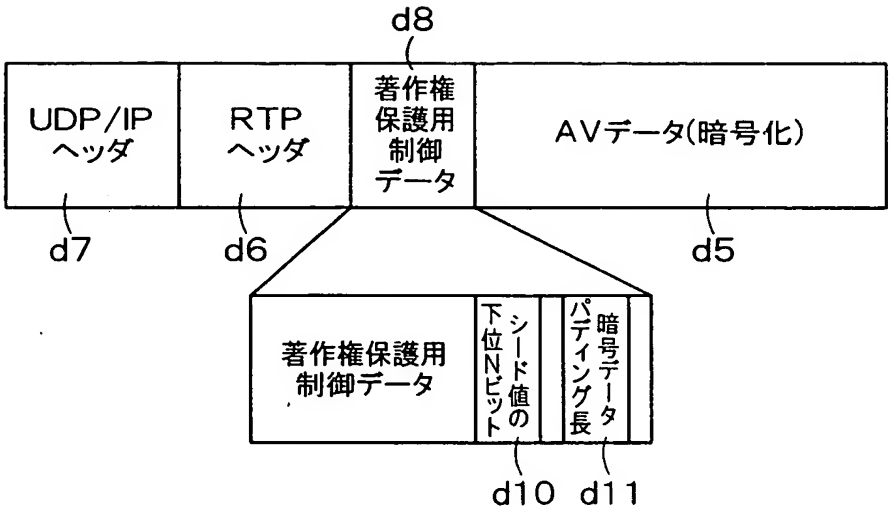
【図５】


d7
d6
d8
d5
UDP/IP
ヘッダ
RTP
ヘッダ
著作権
保護用
制御
データ
AVデータ(暗号化)
RTP
ヘッダ
ペイロード
タイプ
d9

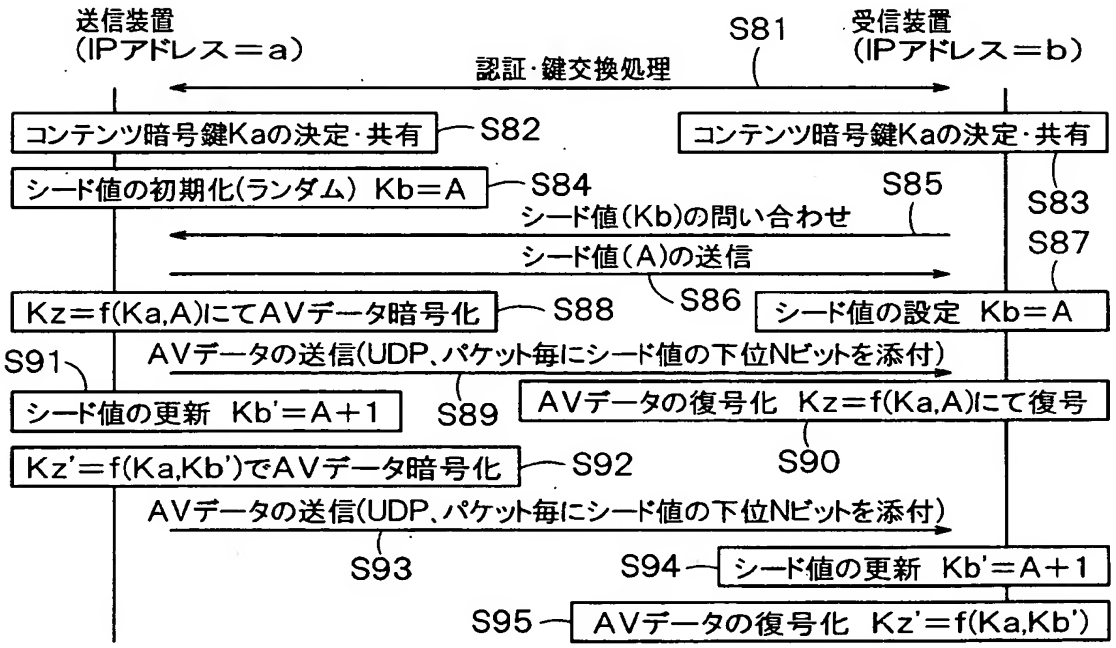
【図６】


送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
AV制御コマンド(再生)(RTSP／TCP／IPにて)
PTのネゴシエーション(PT＝#z)
S1
AVデータ暗号化
S2
AVデータ(暗号化されて)(RTP／IPにて)
(送信ポート番号＝#x、受信ポート番号＝#y、PT＝#z)
S3
認証・鍵交換要求(IPパケット、又はイーサネットフレームにて)
(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、
PT＝#z)のストリームに関して
S4
認証・鍵交換手順(IPパケット、ないし物理レイヤリンクないしレイヤのフレームにて)
S5
S6
復号鍵取得

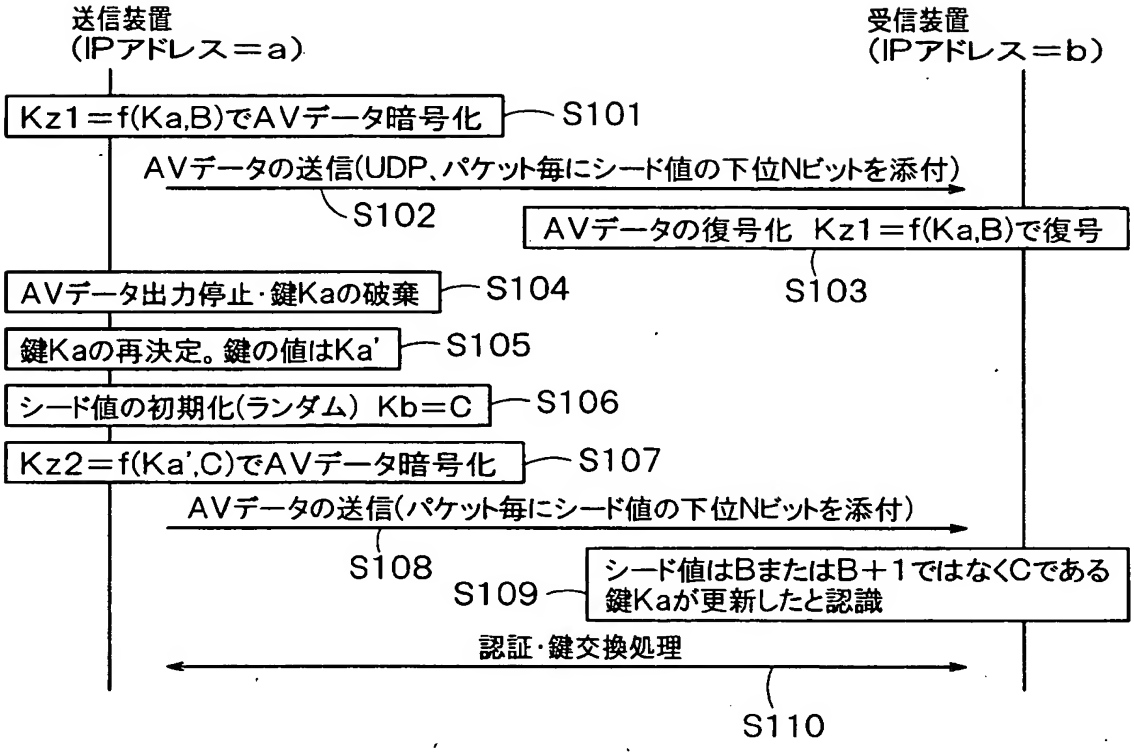
【図７】


d8
UDP/IP
ヘッダ
RTP
ヘッダ
著作権
保護用
制御
データ
AVデータ(暗号化)
d7
d6
d5
著作権保護用
制御データ
シード値の
下位Nビット
パディング長
暗号データ
d10
d11

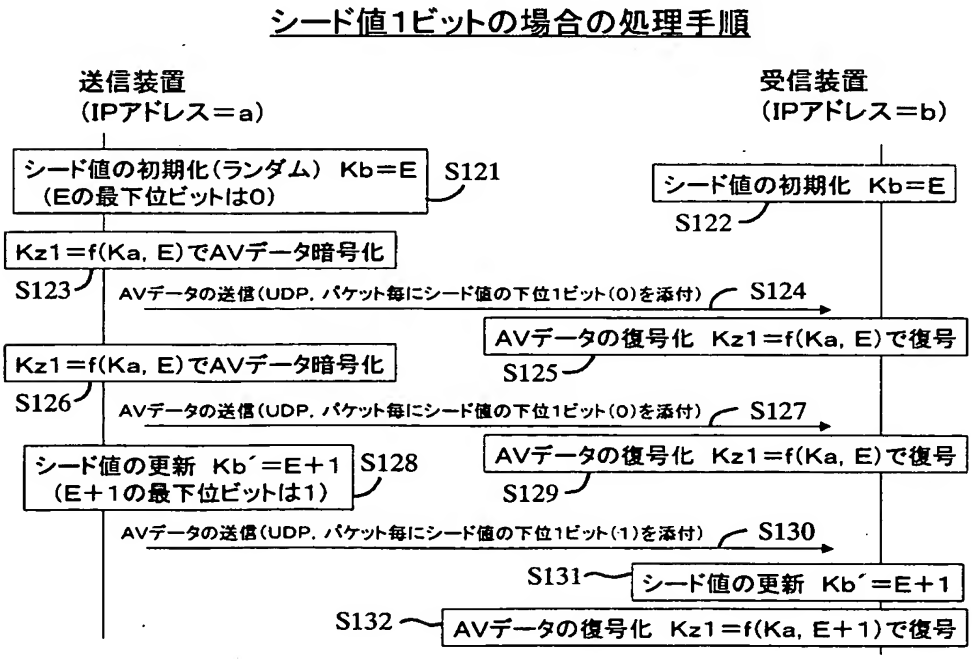
【図８】


送信装置
(IPアドレス＝a)
S81
受信装置
(IPアドレス＝b)
認証･鍵交換処理
コンテンツ暗号鍵Kaの決定･共有
S82
コンテンツ暗号鍵Kaの決定･共有
シード値の初期化(ランダム) Kb＝A
S84
S85
S83
シード値(Kb)の問い合わせ
シード値(A)の送信
S87
Kz＝f(Ka,A)にてAVデータ暗号化
S88
S86
シード値の設定 Kb＝A
S91
AVデータの送信(UDP、パケット毎にシード値の下位Nビットを添付)
シード値の更新 Kb'＝A＋1
S89
AVデータの復号化 Kz＝f(Ka,A)にて復号
Kz'＝f(Ka,Kb')でAVデータ暗号化
S92
S90
AVデータの送信(UDP、パケット毎にシード値の下位Nビットを添付)
S93
S94
シード値の更新 Kb'＝A＋1
S95
AVデータの復号化 Kz'＝f(Ka,Kb')

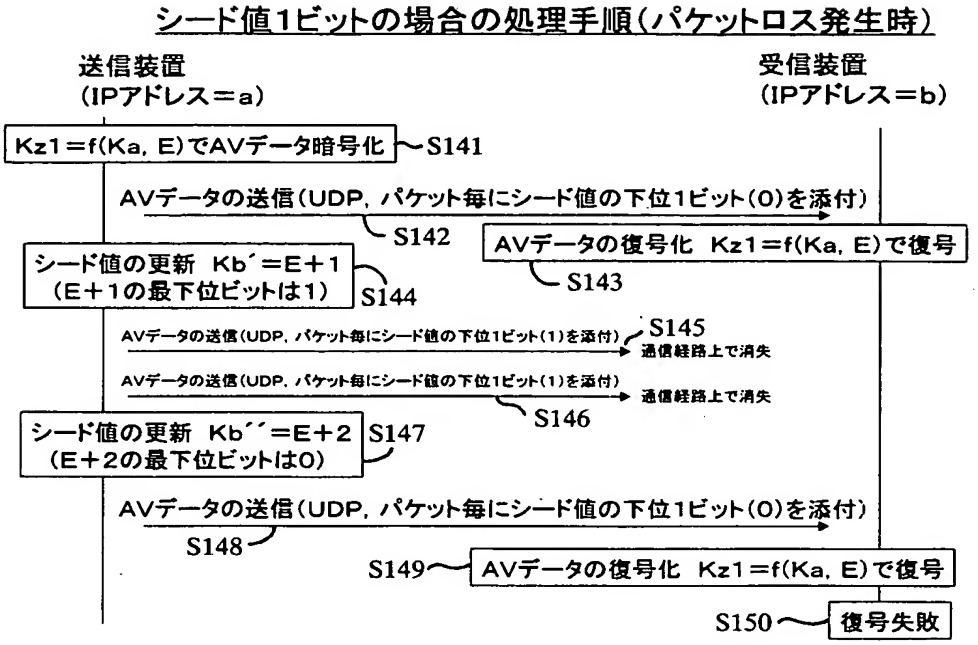
【図９】


送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
Kz1＝f(Ka,B)でAVデータ暗号化
S101
AVデータの送信(UDP、パケット毎にシード値の下位Nビットを添付)
S102
AVデータの復号化 Kz1＝f(Ka,B)で復号
S103
AVデータ出力停止・鍵Kaの破棄
S104
鍵Kaの再決定。鍵の値はKa'
S105
シード値の初期化(ランダム) Kb＝C
S106
Kz2＝f(Ka',C)でAVデータ暗号化
S107
AVデータの送信(パケット毎にシード値の下位Nビットを添付)
S108
S109
シード値はBまたはB＋1ではなくCである
鍵Kaが更新したと認識
認証・鍵交換処理
S110

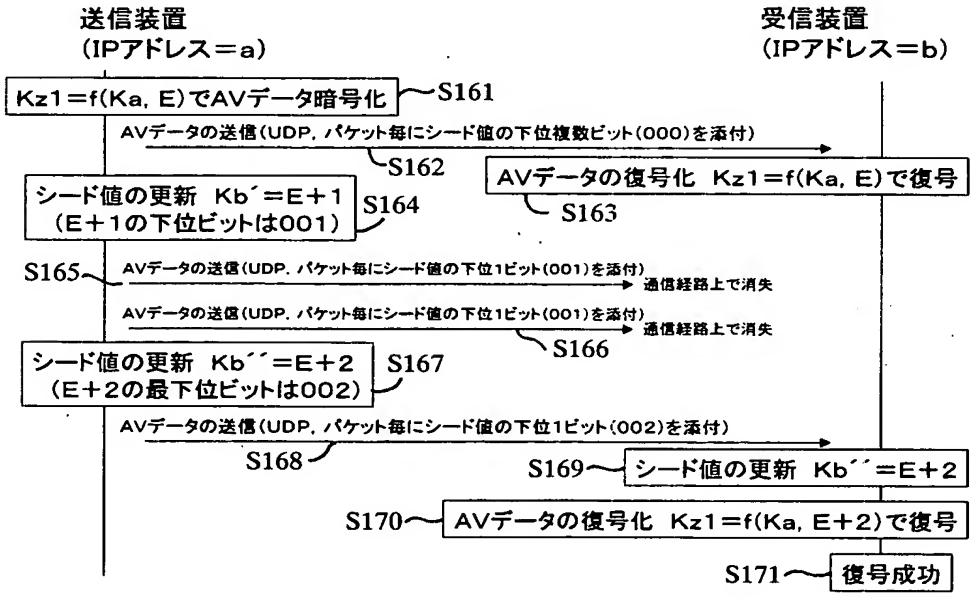
【図１０】


シード値1ビットの場合の処理手順
送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
シード値の初期化(ランダム) Kb＝E
(Eの最下位ビットは0)
S121
シード値の初期化 Kb＝E
S122
Kz1＝f(Ka, E)でAVデータ暗号化
S123
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(0)を添付)
S124
AVデータの復号化 Kz1＝f(Ka, E)で復号
S125
Kz1＝f(Ka, E)でAVデータ暗号化
S126
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(0)を添付)
S127
シード値の更新 Kb'＝E＋1
(E＋1の最下位ビットは1)
S128
AVデータの復号化 Kz1＝f(Ka, E)で復号
S129
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(1)を添付)
S130
S131
シード値の更新 Kb'＝E＋1
S132
AVデータの復号化 Kz1＝f(Ka, E＋1)で復号

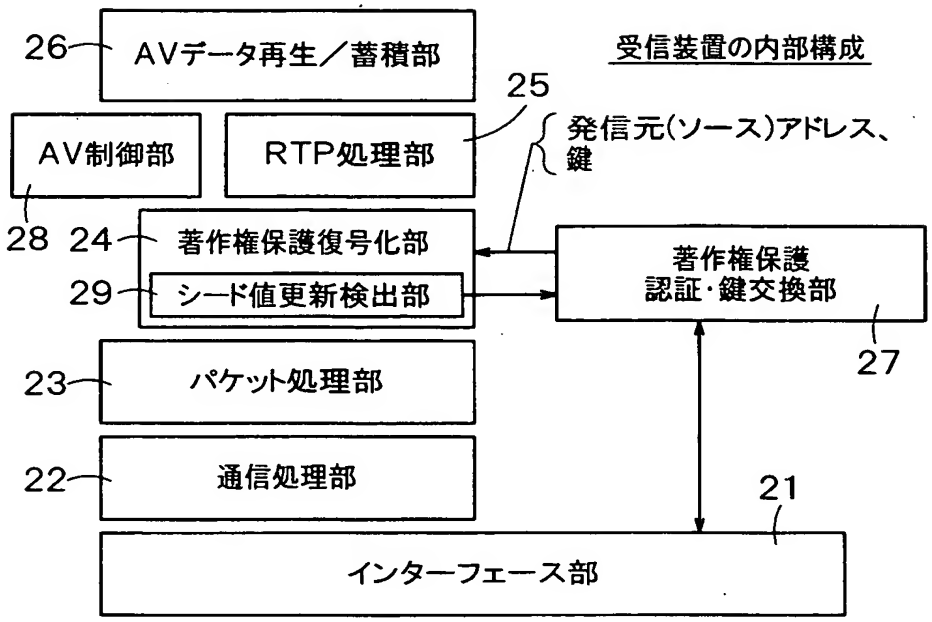
【図１１】


シード値1ビットの場合の処理手順(パケットロス発生時)
送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
Kz1＝f(Ka, E)でAVデータ暗号化
S141
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(0)を添付)
S142
AVデータの復号化 Kz1＝f(Ka, E)で復号
S143
シード値の更新 Kb´＝E＋1
(E＋1の最下位ビットは1)
S144
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(1)を添付)
S145
通信経路上で消失
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(1)を添付)
S146
通信経路上で消失
シード値の更新 Kb´´＝E＋2
(E＋2の最下位ビットは0)
S147
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(0)を添付)
S148
S149
AVデータの復号化 Kz1＝f(Ka, E)で復号
S150
復号失敗

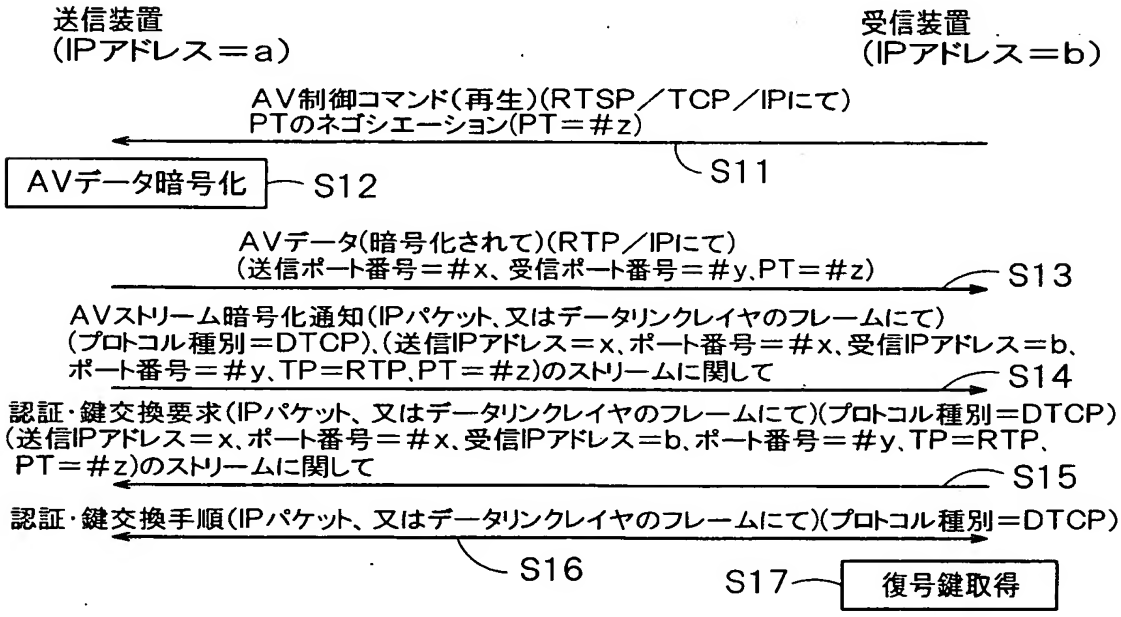
【図１２】


シード値複数ビットの場合の処理手順
送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
Kz1＝f(Ka, E)でAVデータ暗号化
S161
AVデータの送信(UDP, パケット毎にシード値の下位複数ビット(000)を添付)
S162
AVデータの復号化 Kz1＝f(Ka, E)で復号
S163
シード値の更新 Kb´＝E＋1
(E＋1の下位ビットは001)
S164
S165
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(001)を添付)
通信経路上で消失
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(001)を添付)
S166
通信経路上で消失
シード値の更新 Kb´´＝E＋2
(E＋2の最下位ビットは002)
S167
AVデータの送信(UDP, パケット毎にシード値の下位1ビット(002)を添付)
S168
S169
シード値の更新 Kb´´＝E＋2
S170
AVデータの復号化 Kz1＝f(Ka, E＋2)で復号
S171
復号成功

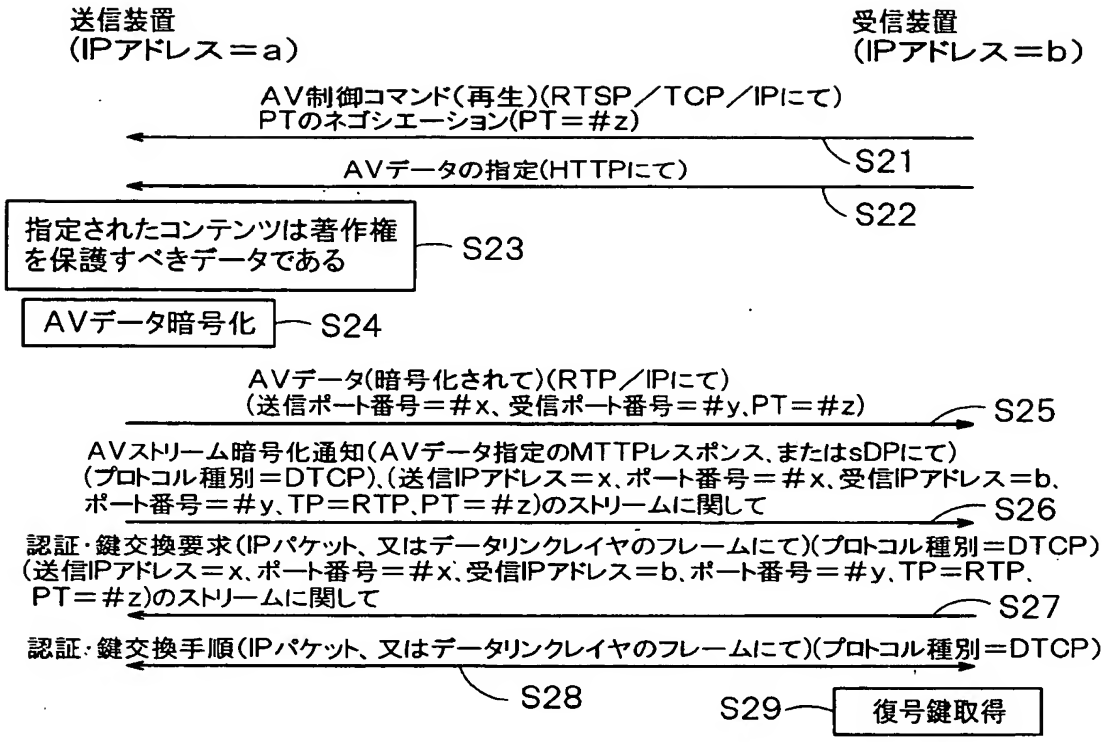
【図１３】


受信装置の内部構成
26
AVデータ再生／蓄積部
25
AV制御部
RTP処理部
発信元(ソース)アドレス、
鍵
28
24
著作権保護復号化部
29
シード値更新検出部
著作権保護
認証・鍵交換部
27
23
パケット処理部
22
通信処理部
21
インターフェース部

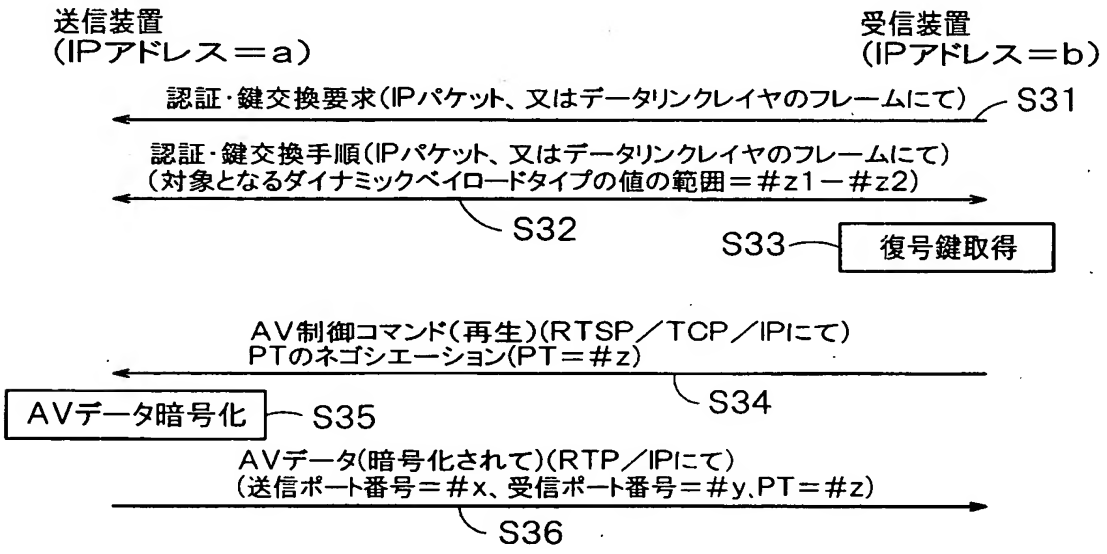
【図１４】


送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
AV制御コマンド(再生)(RTSP／TCP／IPにて)
PTのネゴシエーション(PT＝#z)
S11
AVデータ暗号化
S12
AVデータ(暗号化されて)(RTP／IPにて)
(送信ポート番号＝#x、受信ポート番号＝#y、PT＝#z)
S13
AVストリーム暗号化通知(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S14
認証・鍵交換要求(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、
PT＝#z)のストリームに関して
S15
認証・鍵交換手順(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
S16
S17
復号鍵取得

【図１５】

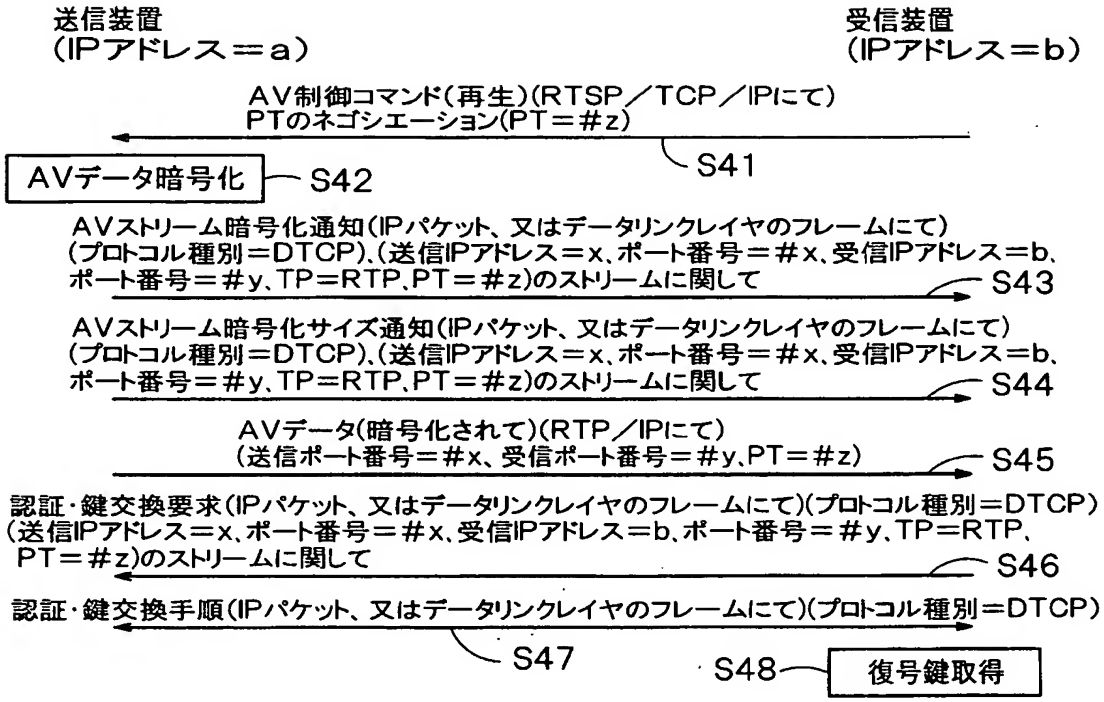


【図１６】

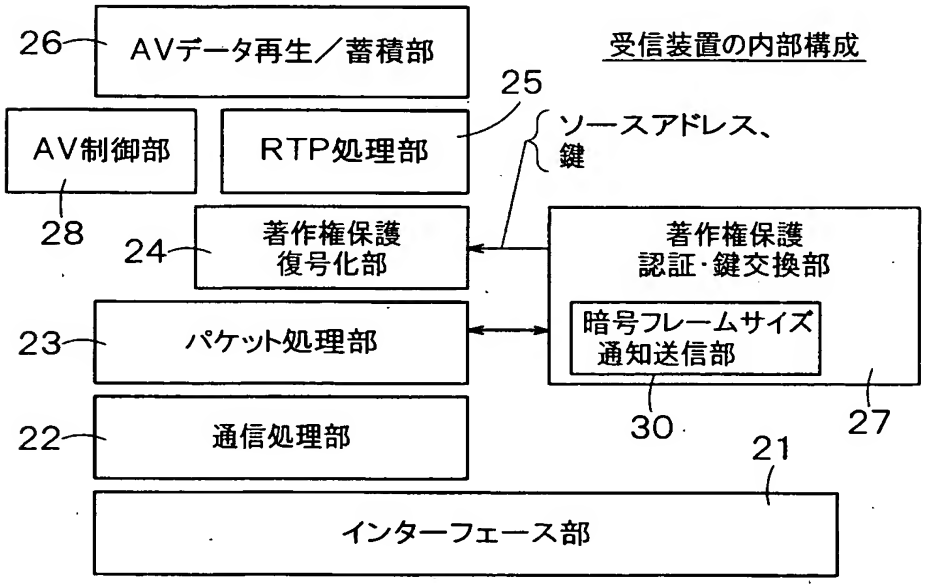


注：(#z1≦#z≦#z2)

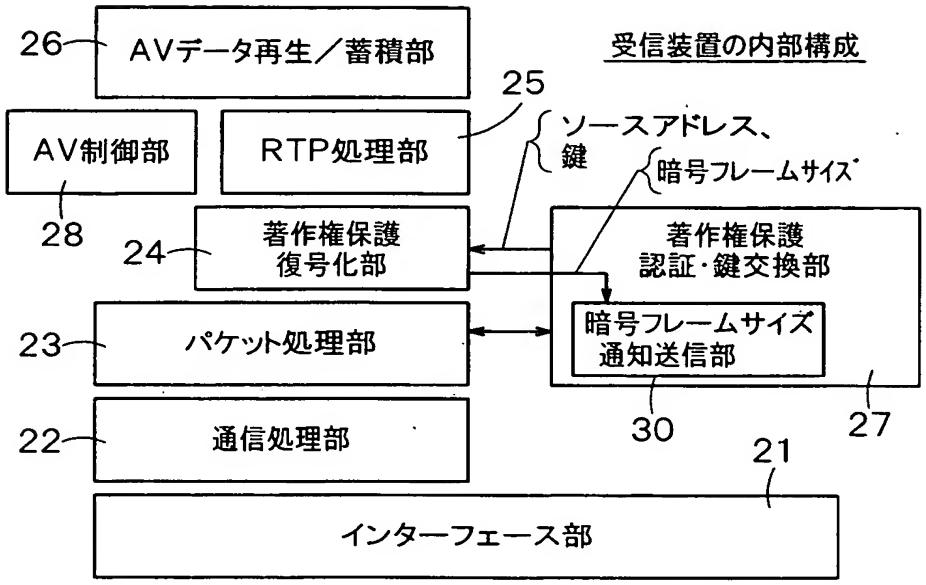
【図１７】


送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
AV制御コマンド(再生)(RTSP／TCP／IPにて)
PTのネゴシエーション(PT＝#z)
S41
AVデータ暗号化
S42
AVストリーム暗号化通知(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S43
AVストリーム暗号化サイズ通知(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S44
AVデータ(暗号化されて)(RTP／IPにて)
(送信ポート番号＝#x、受信ポート番号＝#y、PT＝#z)
S45
認証・鍵交換要求(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、
PT＝#z)のストリームに関して
S46
認証・鍵交換手順(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
S47
S48
復号鍵取得

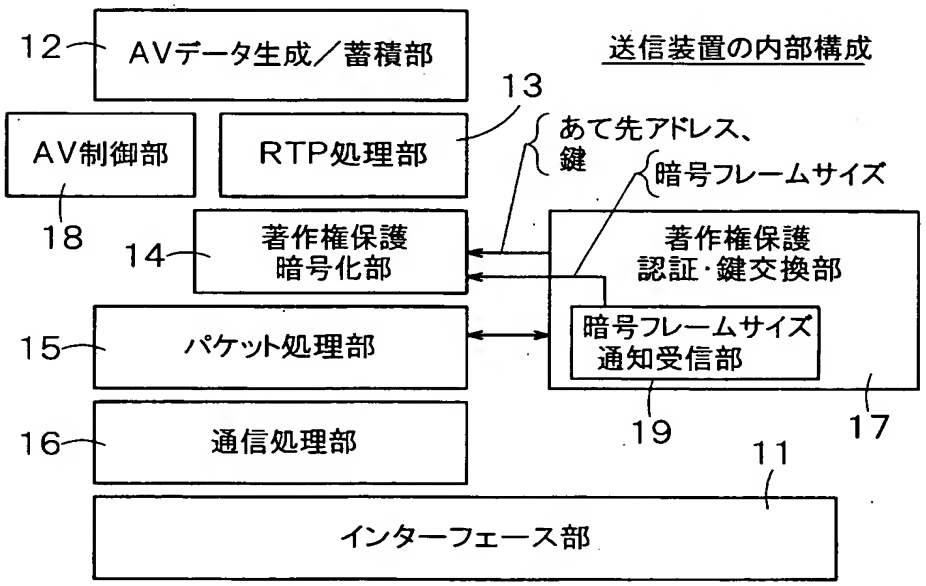
【図１８】


受信装置の内部構成
26
AVデータ再生／蓄積部
25
AV制御部
RTP処理部
ソースアドレス、
鍵
28
24
著作権保護
復号化部
著作権保護
認証・鍵交換部
23
パケット処理部
暗号フレームサイズ
通知送信部
30
27
22
通信処理部
21
インターフェース部

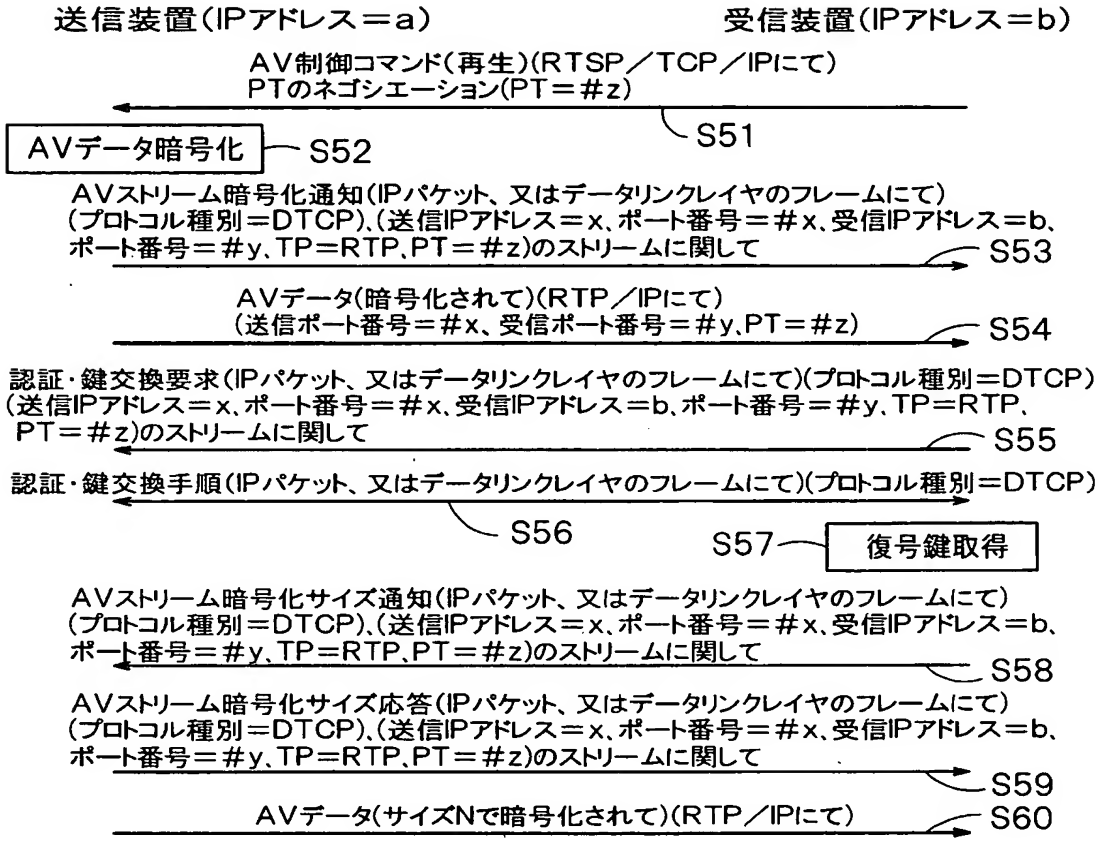
【図１９】


受信装置の内部構成
26
AVデータ再生／蓄積部
25
AV制御部
RTP処理部
ソースアドレス、
鍵
暗号フレームサイズ
28
24
著作権保護
復号化部
著作権保護
認証・鍵交換部
23
パケット処理部
暗号フレームサイズ
通知送信部
22
通信処理部
30
27
21
インターフェース部

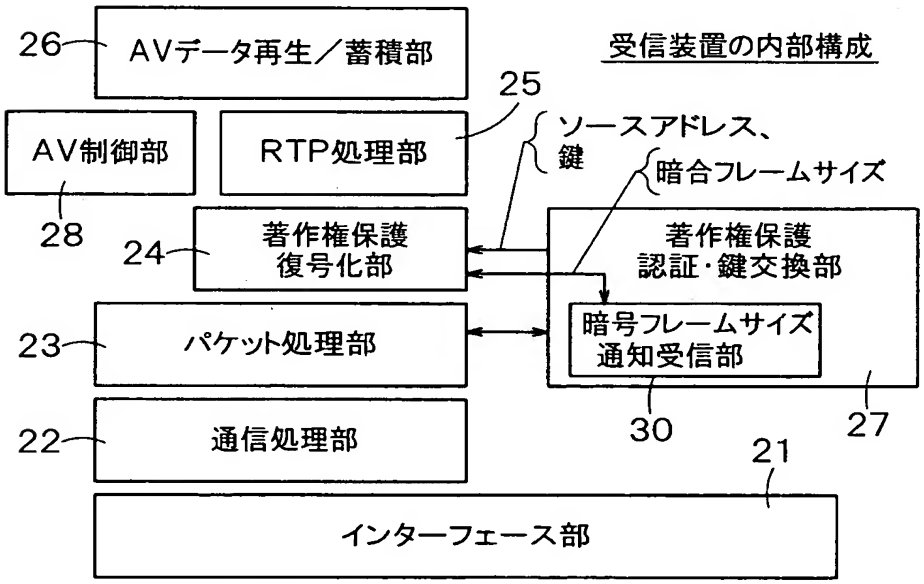
【図２０】


送信装置の内部構成
12
AVデータ生成／蓄積部
13
AV制御部
RTP処理部
あて先アドレス、
鍵
暗号フレームサイズ
18
14
著作権保護
暗号化部
著作権保護
認証・鍵交換部
15
パケット処理部
暗号フレームサイズ
通知受信部
16
通信処理部
19
17
11
インターフェース部

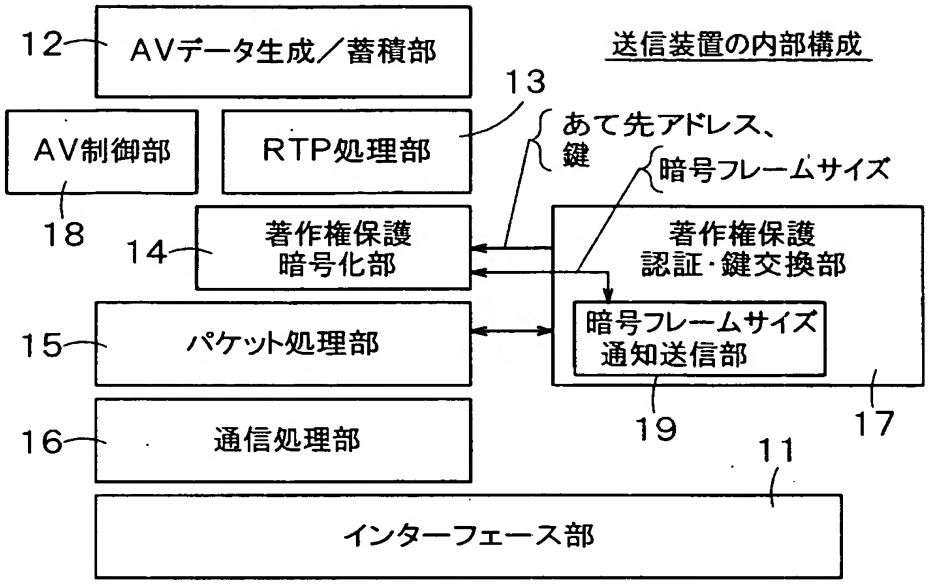
【図２１】


送信装置(IPアドレス＝a)
受信装置(IPアドレス＝b)
AV制御コマンド(再生)(RTSP／TCP／IPにて)
PTのネゴシエーション(PT＝#z)
S51
AVデータ暗号化
S52
AVストリーム暗号化通知(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S53
AVデータ(暗号化されて)(RTP／IPにて)
(送信ポート番号＝#x、受信ポート番号＝#y、PT＝#z)
S54
認証・鍵交換要求(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、
PT＝#z)のストリームに関して
S55
認証・鍵交換手順(IPパケット、又はデータリンクレイヤのフレームにて)(プロトコル種別＝DTCP)
S56
S57
復号鍵取得
AVストリーム暗号化サイズ通知(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S58
AVストリーム暗号化サイズ応答(IPパケット、又はデータリンクレイヤのフレームにて)
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、
ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S59
AVデータ(サイズNで暗号化されて)(RTP／IPにて)
S60

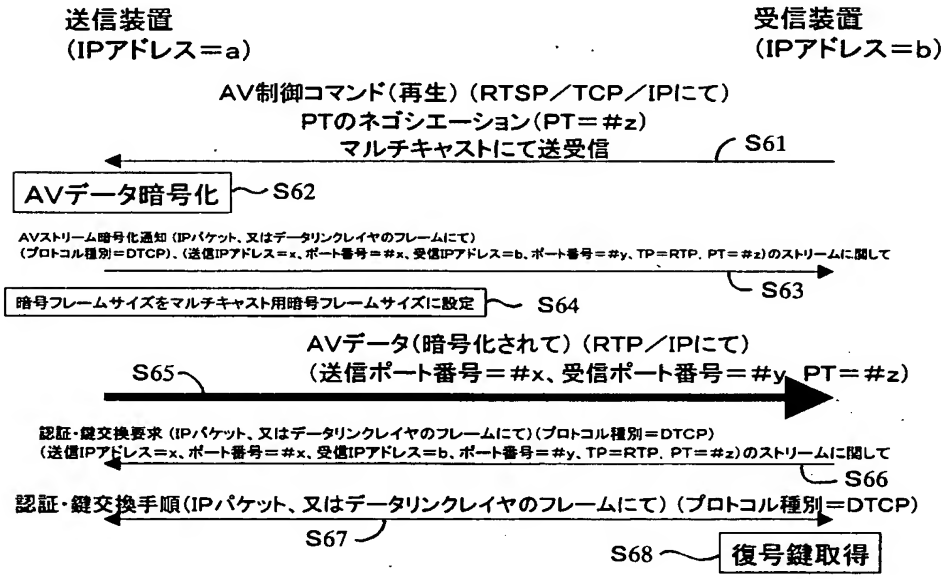
【図２２】


受信装置の内部構成
26
AVデータ再生／蓄積部
25
AV制御部
RTP処理部
ソースアドレス、
鍵
暗合フレームサイズ
28
24
著作権保護
復号化部
著作権保護
認証・鍵交換部
23
パケット処理部
暗号フレームサイズ
通知受信部
22
通信処理部
30
27
21
インターフェース部

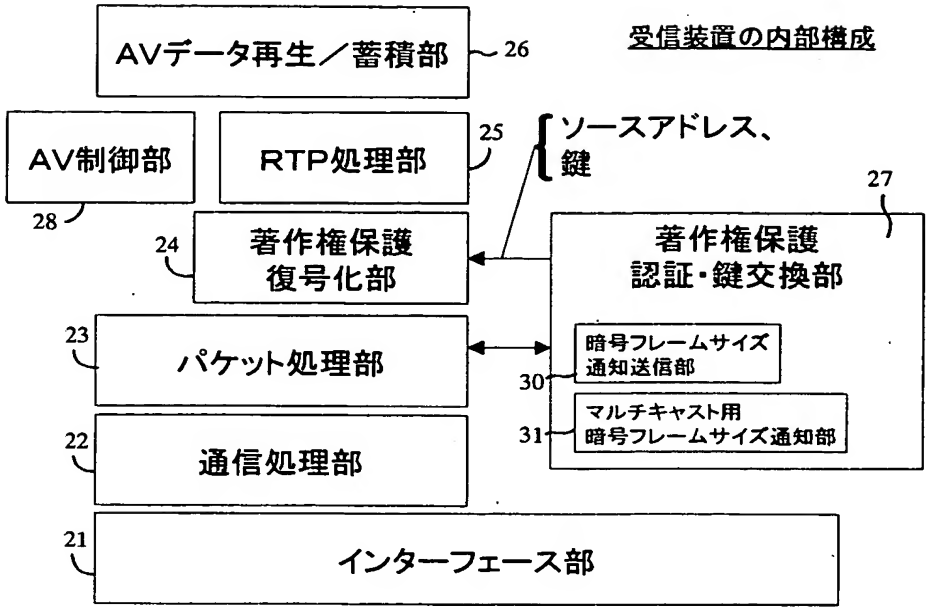
【図２３】


12
AVデータ生成／蓄積部
送信装置の内部構成
13
AV制御部
RTP処理部
あて先アドレス、
鍵
暗号フレームサイズ
18
14
著作権保護
暗号化部
著作権保護
認証・鍵交換部
15
パケット処理部
暗号フレームサイズ
通知送信部
16
通信処理部
19
17
11
インターフェース部

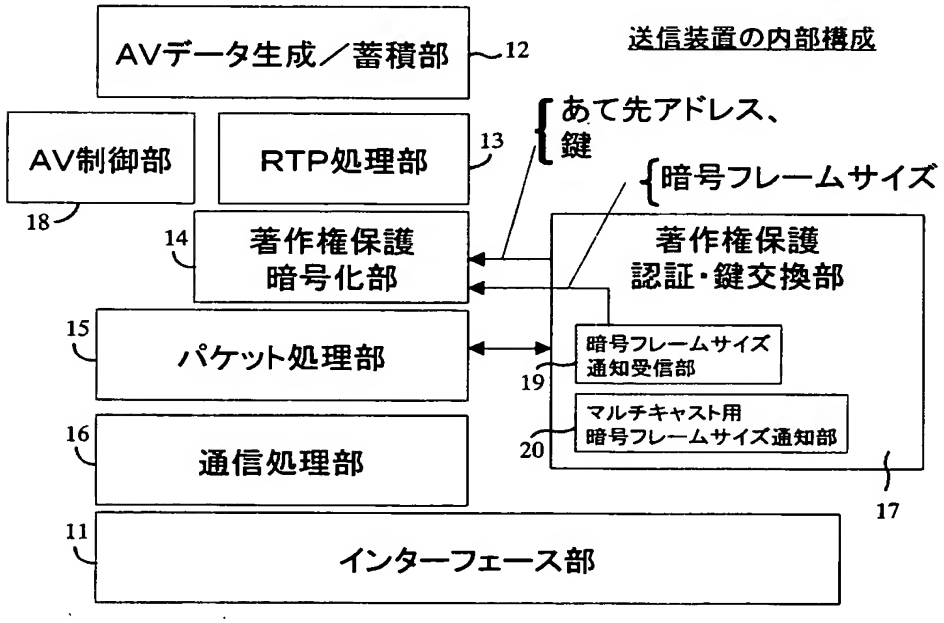
【図２４】


送信装置
(IPアドレス＝a)
受信装置
(IPアドレス＝b)
AV制御コマンド(再生)（RTSP／TCP／IPにて）
PTのネゴシエーション(PT＝#z)
マルチキャストにて送受信
S61
AVデータ暗号化
S62
AVストリーム暗号化通知（IPパケット、又はデータリンクレイヤのフレームにて）
(プロトコル種別＝DTCP)、(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S63
暗号フレームサイズをマルチキャスト用暗号フレームサイズに設定
S64
AVデータ(暗号化されて)（RTP／IPにて）
(送信ポート番号＝#x、受信ポート番号＝#y、PT＝#z)
S65
認証・鍵交換要求（IPパケット、又はデータリンクレイヤのフレームにて）(プロトコル種別＝DTCP)
(送信IPアドレス＝x、ポート番号＝#x、受信IPアドレス＝b、ポート番号＝#y、TP＝RTP、PT＝#z)のストリームに関して
S66
認証・鍵交換手順(IPパケット、又はデータリンクレイヤのフレームにて)（プロトコル種別＝DTCP）
S67
S68
復号鍵取得

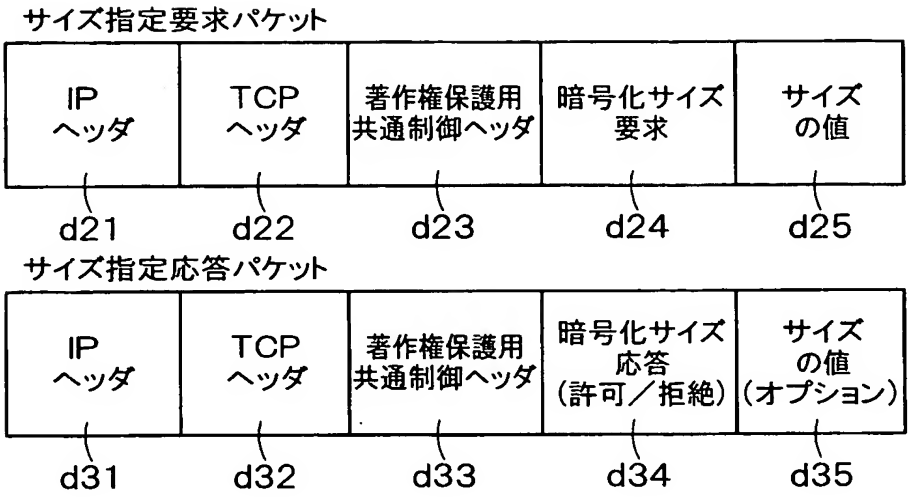
【図２５】


受信装置の内部構成
AVデータ再生／蓄積部
26
AV制御部
RTP処理部
25
ソースアドレス、
鍵
27
28
24
著作権保護
復号化部
著作権保護
認証・鍵交換部
23
パケット処理部
暗号フレームサイズ
通知送信部
30
マルチキャスト用
暗号フレームサイズ通知部
31
22
通信処理部
21
インターフェース部

【図２６】


送信装置の内部構成
AVデータ生成／蓄積部
12
あて先アドレス、
鍵
AV制御部
RTP処理部
13
暗号フレームサイズ
18
14
著作権保護
暗号化部
著作権保護
認証・鍵交換部
15
パケット処理部
暗号フレームサイズ
通知受信部
19
マルチキャスト用
暗号フレームサイズ通知部
20
16
通信処理部
17
11
インターフェース部

【図２７】


サイズ指定要求パケット
IP ヘッダ
TCP ヘッダ
著作権保護用 共通制御ヘッダ
暗号化サイズ 要求
サイズ の値
d21
d22
d23
d24
d25
サイズ指定応答パケット
IP ヘッダ
TCP ヘッダ
著作権保護用 共通制御ヘッダ
暗号化サイズ 応答 (許可／拒絶)
サイズ の値 (オプション)
d31
d32
d33
d34
d35

【書類名】　要約書

【要約】

【課題】　著作権保護を図りつつ電子データの送信または受信を行えるようにする。

【解決手段】　AV通信システムは、ある家庭内のホームネットワーク１と、このホームネットワーク１に接続されている送信装置２及び受信装置３とを備えている。著作権保護の必要なAVデータを暗号化したペイロードに、プロトコル種別（例えばRTP）と、このプロトコルが使用するペイロードタイプの値と、を付加したAVストリームを送信装置２から受信装置３に送信するため、このAVストリームを受信した受信装置３は、AVデータが暗号化されていることを容易に検出でき、かつ認証・鍵交換が必要なデータを容易に識別できる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１７３９８５
受付番号	５０３０１０１９９９９
書類名	特許願
担当官	第一担当上席　　００９０
作成日	平成１５年　６月２３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000003078

【住所又は居所】　東京都港区芝浦一丁目１番１号

【氏名又は名称】　株式会社東芝

【代理人】　申請人

【識別番号】　100075812

【住所又は居所】　東京都千代田区丸の内３－２－３　協和特許法律事務所

【氏名又は名称】　吉武　賢次

【選任した代理人】

【識別番号】　100088889

【住所又は居所】　東京都千代田区丸の内３丁目２番３号　協和特許法律事務所

【氏名又は名称】　橘谷　英俊

【選任した代理人】

【識別番号】　100082991

【住所又は居所】　東京都千代田区丸の内３丁目２番３号　富士ビル　協和特許法律事務所

【氏名又は名称】　佐藤　泰和

【選任した代理人】

【識別番号】　100096921

【住所又は居所】　東京都千代田区丸の内３－２－３　富士ビル３階　協和特許法律事務所

【氏名又は名称】　吉元　弘

【選任した代理人】

【識別番号】　100103263

【住所又は居所】　東京都千代田区丸の内３丁目２番３号　協和特許法律事務所

次頁有

認定・付加情報（続き）

【氏名又は名称】　川崎　康

次頁無

特願２００３－１７３９８５

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝